

AD-A271 877



Technical Document 2499
August 1993

Understanding Open Systems Interconnection (OSI)

G. B. Myers



93-27187

93-27187



Approved for public release; distribution is unlimited.



80

3

Technical Document 2499

August 1993

Understanding Open Systems Interconnection (OSI)

G. B. Myers

NAVAL COMMAND, CONTROL AND
OCEAN SURVEILLANCE CENTER
RDT&E DIVISION
San Diego, California 92152-5001

K. E. EVANS, CAPT, USN
Commanding Officer

R. T. SHEARER
Executive Director

ADMINISTRATIVE INFORMATION

This work was performed by members of the Information Processing and Displaying Division, Naval Command, Control and Ocean Surveillance Center, RDT&E Division, San Diego, CA 92152-5001.

Released by
G. B. Myers,
Associate

Under authority of
A. G. Justice, Head
Information Processing
and Displaying Division

DTIC QUALITY INSPECTED 8

Accession For	
NTIS GRA&I	<input checked="" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By _____	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

MA

CONTENTS

INTRODUCTION	1
WHAT IS OSI?	1
BACKGROUND	2
WHAT IS THE OSI STANDARDS PROCESS?	2
WHAT IS THE OSI REFERENCE MODEL?	4
PROTOCOLS	5
WHAT IS THE GOVERNMENT OSI PROFILE (GOSIP)?	8
WHAT IS SAFENET?	10
WHERE IS LAN TECHNOLOGY HEADED?	13
CONCLUSION	14
REFERENCES	15
BIBLIOGRAPHY	15
GLOSSARY	17

FIGURES

1. Interconnecting networks.	1
2. The OSI standards process.	3
3. OSI reference model layers.	4
4. OSI reference model layer functions.	4
5. OSI reference model layer operations.	5
6. Protocols—frame construction.	6
7. Wide area network example.	7
8. GOSIP version 2.	8
9. Networked connections with SAFENET.	10
10. SAFENET profile.	11
11. SAFENET topology.	12
12. LAN technology trends.	13

INTRODUCTION

Open Systems Interconnection (OSI) is a nonproprietary and "open" approach to communications between different types of computers. OSI is a data communications concept "whereby computer systems are able to communicate in an open environment without knowledge of specific characteristics of remote computers." (reference 1) The Naval Command, Control and Ocean Surveillance Center, RDT&E Division (NRaD) is using OSI in developing new Navy computer systems and has participated in standards development.

More than 80 separate specifications make up OSI standards. This paper is a guide for people who are new to the OSI concepts. We have defined terminology and described concepts that are important to achieving a better understanding of OSI. We will answer the following questions:

1. What is OSI?
2. What is the OSI standards process?
3. What is the OSI reference model?
4. What is the Government OSI Profile (GOSIP)?
5. What is Survivable Adaptable Fiber-optic Embedded Network (SAFENET)?
6. Where is Local Area Network (LAN) technology headed?

WHAT IS OSI?

OSI is a joint standardization program supported by both the International Standards Organization (ISO) and the Consultative Committee for International Telephone and Telegraph (CCITT). The purpose of the OSI program is to support the networking of information processing computer systems on a worldwide basis. OSI establishes a set of nonproprietary and open international standards to facilitate open interconnection among different types of computer systems. Often this networking is accomplished using switched telephone networks. See figure 1.

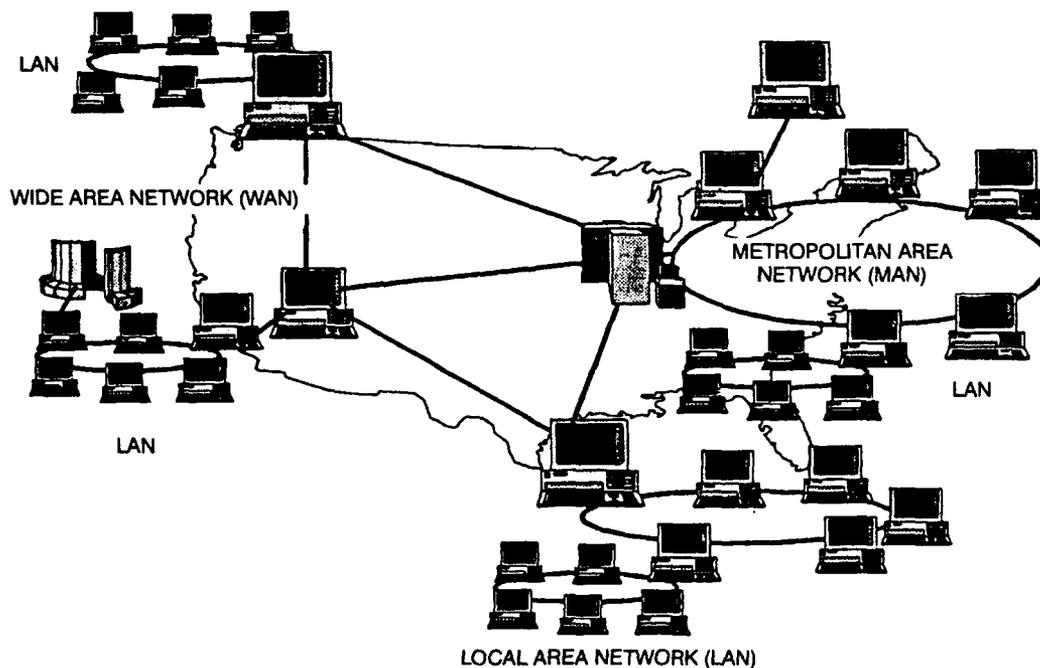


Figure 1. Interconnecting networks.

BACKGROUND

During the 1960s and 1970s computer vendors such as International Business Machines (IBM) and Digital Equipment Corporation (DEC) established proprietary computer communications protocols to enable mainframe computers and minicomputers to interconnect and exchange information. Networking standards and products such as IBM's Systems Network Architecture (SNA) and DEC's DECNET enabled information management organizations to move information between computers that complied with these proprietary ("closed") communications protocols. These computer networks are highly successful. Private, proprietary network technologies link thousands of computers together. The introduction of the personal computer in the early 1980s created tremendous growth in Local Area Networks (LANs). Wide Area Networks (WANs) have evolved to interconnect the LANs to create international computer connectivity.

Two nonproprietary sets of communication protocols were developed in the 1970s and 1980s: (1) Internet (known originally as ARPANET) and (2) OSI. The first to be implemented was Internet's predecessor, ARPANET, which was originally developed by the Department of Defense (DoD) Advanced Research Projects Agency (DARPA) as a way of interconnecting DoD computers. Internet has grown to become an extremely valuable communications support network providing connections to many organizations within and outside of DoD.

The second set of nonproprietary protocols to emerge has been the ISO standards commonly known as OSI. OSI has taken significantly longer in the standards-formation process due to the extensive number of nations, organizations, and individuals who have been involved. Internet development was more focused due to an ability to constrain the problem (Internet protocols support text transmission, primarily) and limit the contributors to the solution (DoD, initially). OSI is a more comprehensive set of networking standards and protocols.

Currently, Internet protocol implementation is a practical network communications solution with many software and hardware products to support users. OSI products are being developed and are readily available to support communications requirements (particularly in Europe).

WHAT IS THE OSI STANDARDS PROCESS?

Standards are essential to many areas of technology and commerce such as construction, photography, air travel, automotive engineering, postal service, and monetary policy. Examples of these standards are fire safety standards in construction (smoke detection and fire protection), film sizes and emulsion speed standards in photography, safety and maintenance standards for commercial aircraft, and telephone standards for worldwide telephone service.

OSI standards are developed and maintained by a number of international and U.S.-based standards organizations. Within the U.S. the following organizations contribute to OSI development:

- The American National Standards Institute (ANSI)
- The National Institute of Standards and Technology (NIST)
- The Institute of Electrical and Electronics Engineers (IEEE)
- The U.S. State Department

As illustrated in figure 2, ANSI committee representatives communicate directly with ISO regarding OSI standards issues. Likewise, representatives of the U.S. State Department maintain contact with CCITT. CCITT, headquartered in Geneva, Switzerland, is a UN affiliated organization that sets tariffs and standards for international telephone communications. ISO is strictly, as its name implies, a standards organization supported by standards bodies from various nations such as France's AFNOR, Britain's BSI, and ANSI. Both ISO and CCITT receive input for standards from the European Computer Management Association (ECMA).

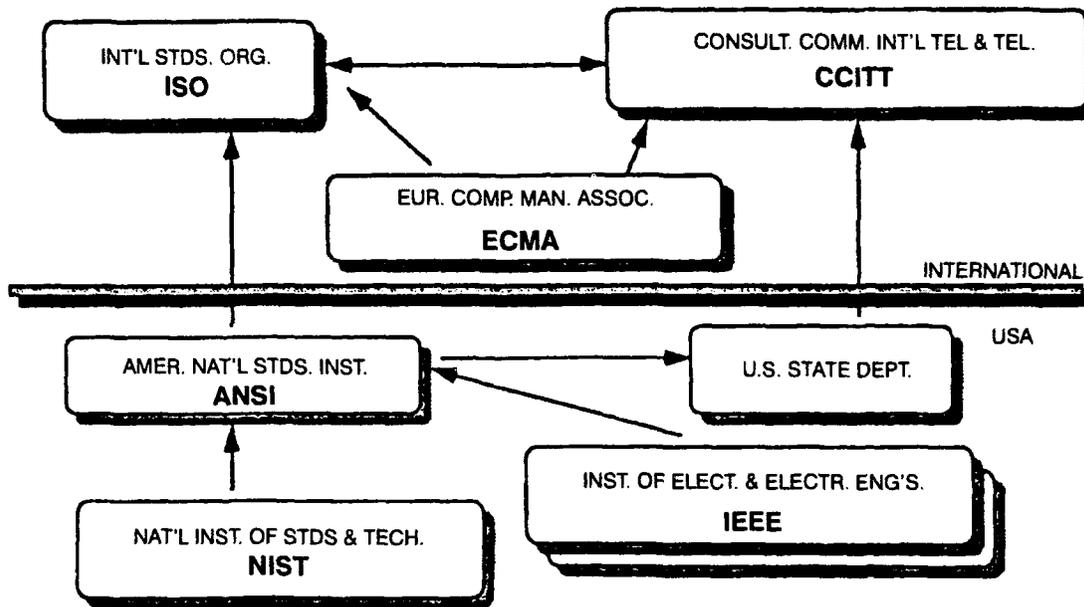


Figure 2. The OSI standards process.

Most standards decisions are reached by consensus or compromise. In some cases, multiple standards are implemented to incorporate versions that are acceptable to the negotiating parties. European participants often develop or support standards with some "looseness" in the specifications, allowing for some latitude in implementation.

Standards then evolve based on commonality or on the best solutions. Participation in the standards process and compliance with the standards is completely voluntary. Generally, compliance is considered to be an advantage to participating organizations unless there is a specific requirement that indicates a need to deviate.

WHAT IS THE OSI REFERENCE MODEL?

The OSI Reference Model defines the functions that have to be performed in sending or receiving messages between computers. Often referred to in technical literature as the “seven-layer” model, it is the most widely known element of the OSI concept! (see figure 3). Definition of the model began in the 1970s and became a standard in the early 1980s. These functions in the model are represented in hierarchical layers.

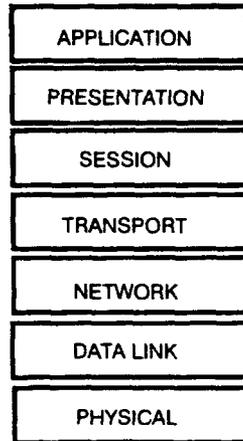


Figure 3. OSI reference model layers.

“The notion of layering embodies a few powerful concepts. Each protocol layer provides a set of services to its user in the next higher layer by building on the services provided to it by the next lower layer. Layers are defined in such a way similar functions are grouped together and interactions across layer boundaries are minimized.”

—T. C. Bartee (reference 2)

Each layer can be implemented separately and changed as long as the service requirements above and below are met. Services are passed up to the layer above and performed by the layer below. Protocols establish the methods of passing data between peer levels within the model. Figure 4 shows the OSI reference model layer functions.

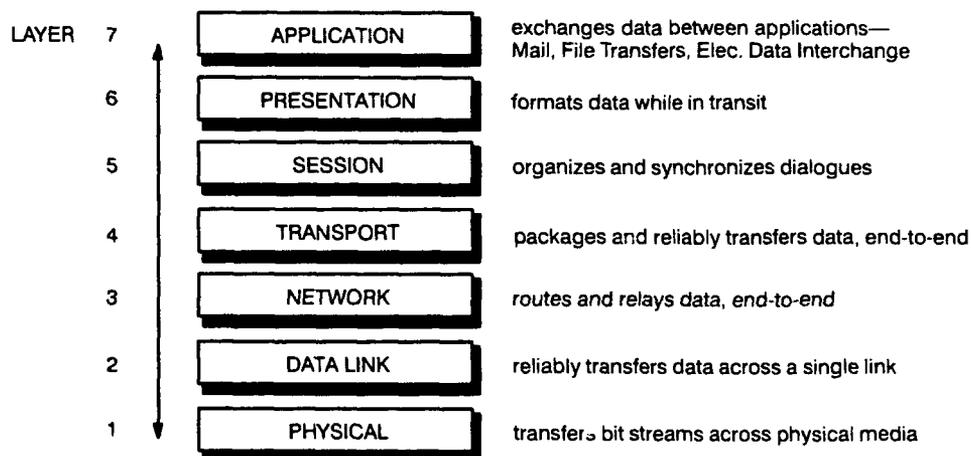


Figure 4. OSI reference model layer functions.

The top three layers of the model: the Application, Presentation, and Session layers, set up standards for supporting the application within the computer. The lower four layers of the model: the Transport, Network, Data Link, and Physical layers, are standards for supporting network communications. Figure 5 shows the OSI reference model layer operation.

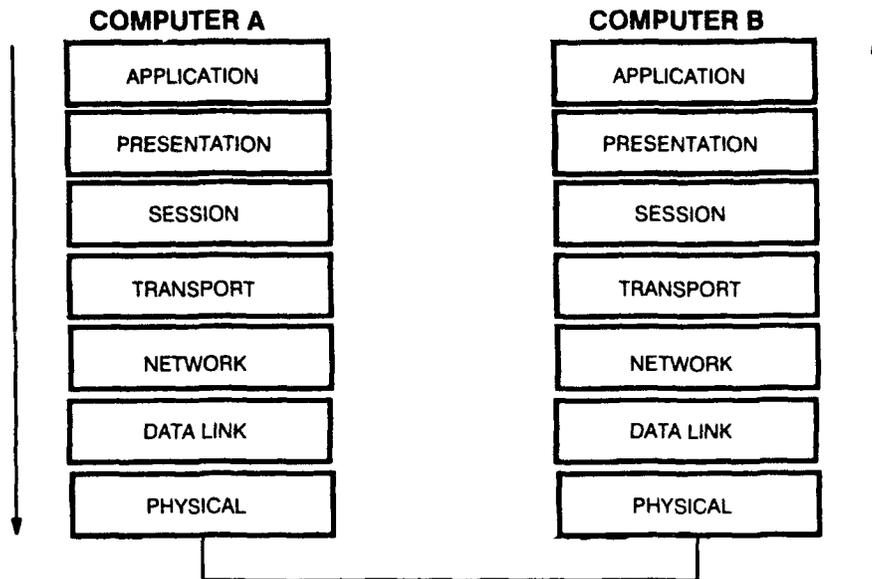


Figure 5. OSI reference model layer operations.

PROTOCOLS

An implementation of computer-to-computer communication employing the OSI model will consist of a protocol or message format for each layer to process and exchange information. The protocol is a specification of what to do, when to do it, and in what format it should be done. The word "protocol" originates from Greek where it referred to an index which was glued on the front cover of a papyrus. This has a direct parallel with the header data and trailer data that are "glued" on to data in the layered network communications process in OSI-based operations.

Protocols define a number of things with respect to intercomputer communications including:

- circuit voltage (0 or 1)
- bit sequences
- data formats
- procedures and rules for certain conditions and actions
- report required under certain conditions

The protocol defines the behavior of the network at each layer—what is allowed and not allowed, permitted actions, and actions that result from conditions that are not met. Protocols are used to establish physical connectivity and to define the process for the exchange of data across the network between applications.

Frame construction is a process of adding information that is meaningful to each layer of the model at the point of origin, and, conversely, stripping this information away at the destination (see figure 6). A frame, the data that are physically passed via the communications media, will potentially have meaningful information to each layer of the model. The application, which is oriented to processing the application data, will not receive the header and trailer information from the Data Link, Network, Transport, Session, and Presentation layers. This information will have been removed by previous layers by the time the application sees the data.

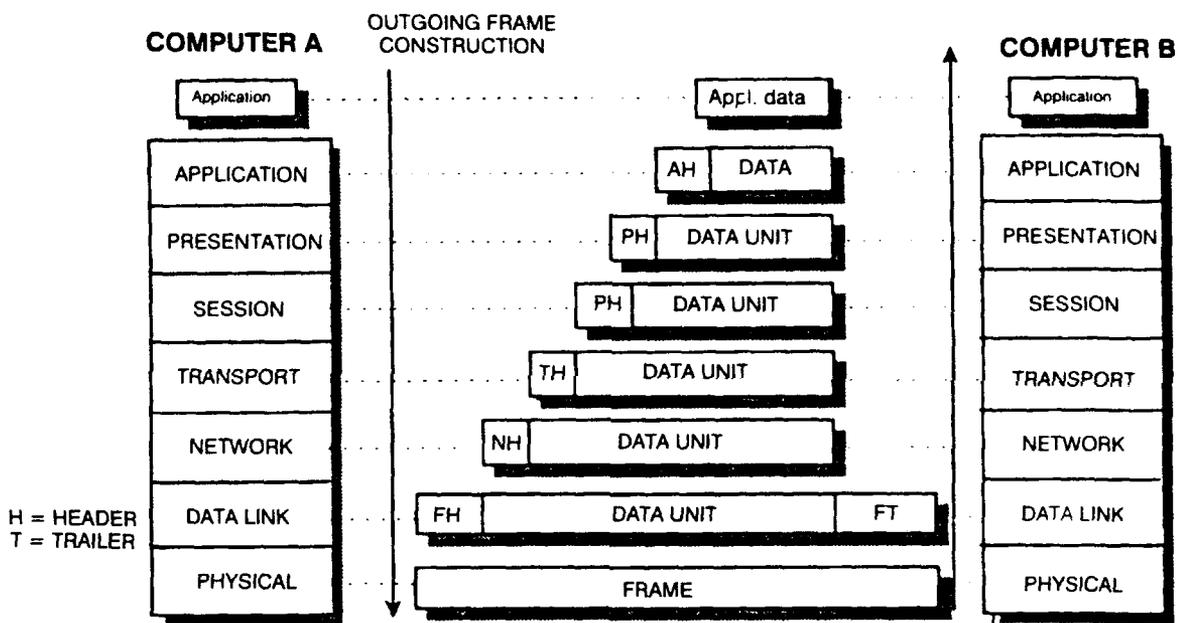


Figure 6. Protocols—frame construction.

In an example of exchanging data across a wide area network, information is passed along via four or more computers prior to its arrival and use in an application. The data are sent by an application and handled by all seven layers of the model in the initiating computer. The network-oriented layers of the protocol are activated in each of the interim computers—computers connected to a wide area network. The destination computer, connected to a local area network, receives the data and employs appropriate layers of the model to deliver the data to the receiving application. Figure 7 is an example of wide area network.

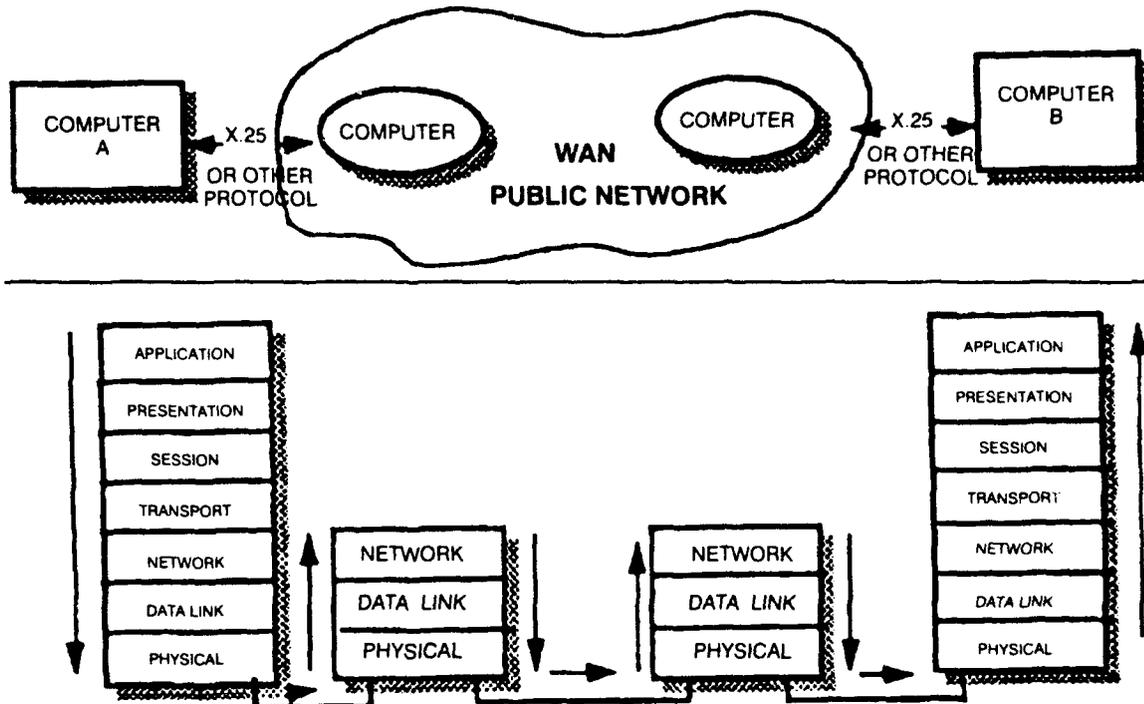


Figure 7. Wide area network example.

WHAT IS THE GOVERNMENT OSI PROFILE (GOSIP)?

The U.S. Government has decided to adopt OSI standards as mandatory for information computer systems. A subset of the OSI standards was selected by the government to become the Government Open Systems Interconnection Profile (GOSIP). A profile is a specific selection of protocols. Figure 8 shows the protocols that make up each layer for the GOSIP.

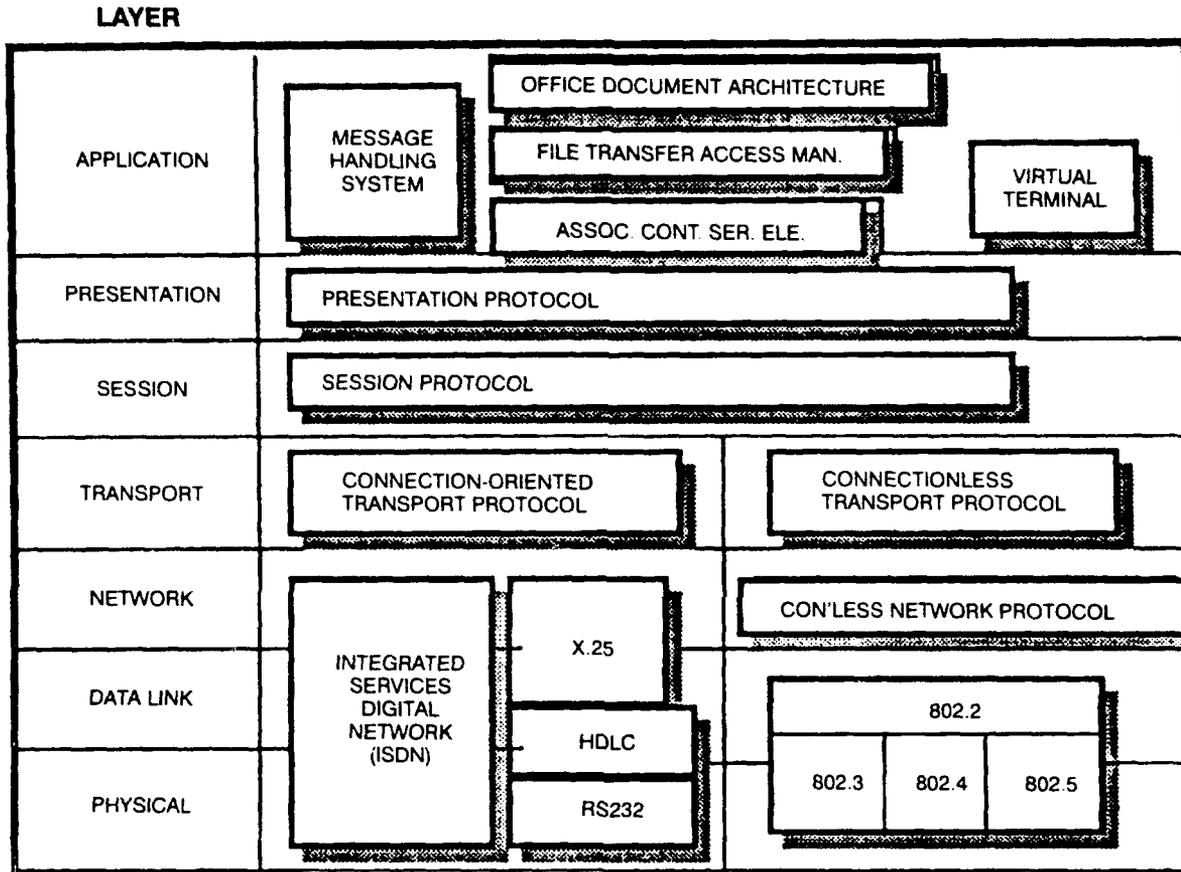


Figure 8. GOSIP version 2.

GOSIP is a selected set of OSI standards and protocols Federal agencies can use to purchase OSI-based products that meet their intercomputer communications requirements. GOSIP is intended to assist users who have little or no experience in OSI implementations or acquisitions and to simplify and ease the process of assimilating OSI technology into Federal agencies. The primary users of GOSIP specifications will be Federal procurement specialists, Federal technical specialists, and Federal managers.

The GOSIP specifications are to

1. Provide for a common generic set of requirements (to avoid having users independently consult a large volume of complex standards).
2. Ensure stability in OSI material referenced in Federal procurements.

The first version of GOSIP became a Federal Information Processing Standard (FIPS 146) in 1988. OSI compliant network connectivity is required in the acquisition of new Government information systems as of FY 1991. GOSIP version 2 was published in 1992, adding facilities for Office Document Architecture (ODA) and the Integrated Service Digital Network (ISDN). GOSIP standards are updated about every 18 months to 2 years. GOSIP version 3 is under development.

The ISDN functions included in GOSIP provide worldwide, high-speed, high-bandwidth digital telecommunications services that integrate voice, fax, digital, and video data. LAN technologies are represented in the lower layers of the GOSIP specifications by IEEE standards 802.3 (Ethernet), 802.4 (Token Bus) and 802.5 (Token Ring). The uppermost layer of the GOSIP specifications, the application layer, accommodates standards for message handling, virtual terminal services, and file transfer.

WHAT IS SAFENET?

“The SAFENET (Survivable Adaptable Fiber-Optic Embedded Network) program is an effort by the U.S. Navy to develop standard computer network profiles which meet the requirements of Navy shipboard mission-critical computer systems. The SAFENET standards are the product of a joint Navy–industry working group, which works in open forum to achieve consensus on all technical issues.”

—J. L. Paige (reference 3)

Currently, the computer systems on most Navy ships are directly linked on a point-to-point basis with special interfaces for each connection. As the number of computers increases, the required number of communication links increases dramatically. SAFENET is a survivable networking technology that reduces the number and weight of the cables on the ship and increases the flexibility and standardization of the computer network. Figure 9 shows the current practice of point-to-point system communications and networked connections with SAFENET.

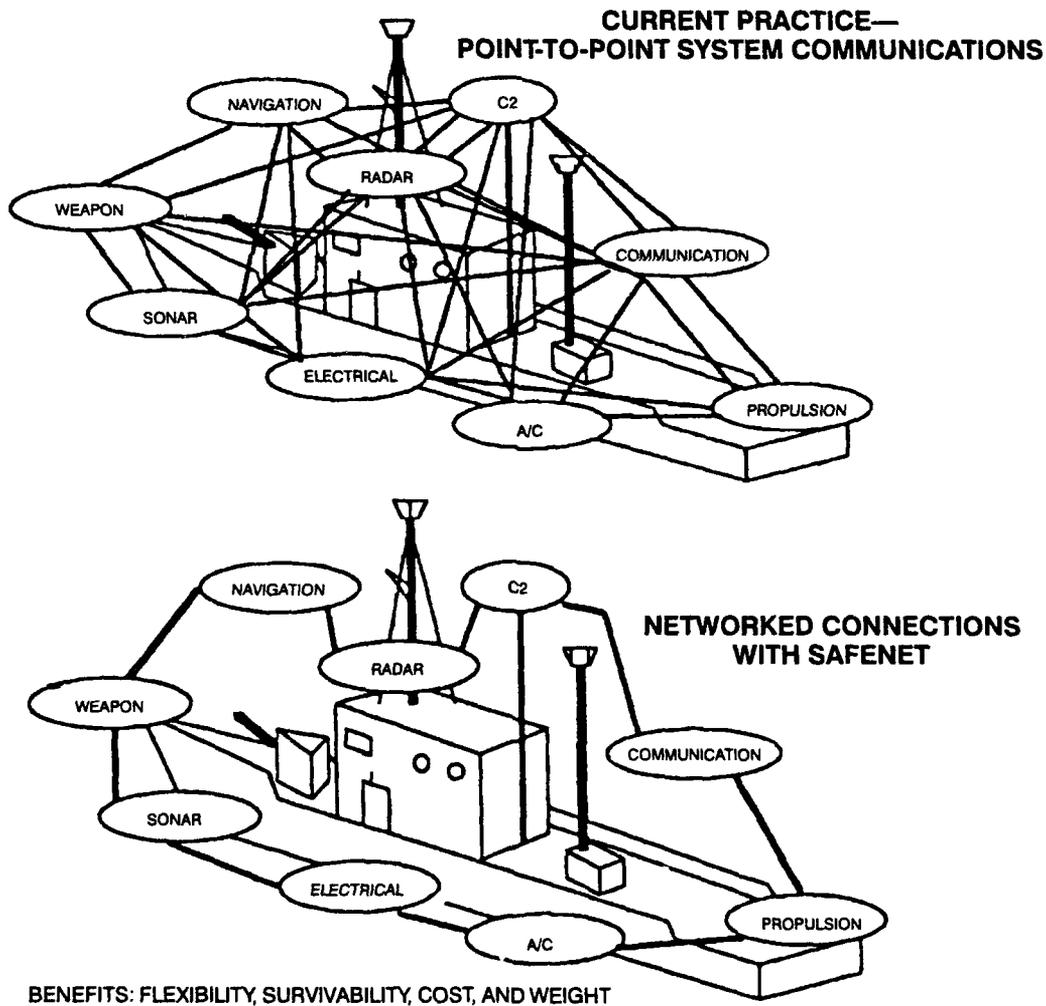


Figure 9. Networked connections with SAFENET.

SAFENET is a protocol profile based on OSI standards that will be available from commercial vendors. It employs the layered protocol architecture prescribed in the OSI reference model. The SAFENET physical and data link layers are based on the ANSI FDDI LAN which operates at 100 Mbps.

Two profiles are available in SAFENET to support OSI compliant networking and realtime data transfer. Realtime data transfer is supported by the SAFENET-specific service definition for "lightweight" support service, which is called the Lightweight Protocol Suite. This protocol suite permits efficient access to the underlying transfer services such as the low-latency Xpress Transfer Protocol (XTP). The SAFENET profile is depicted in figure 10.

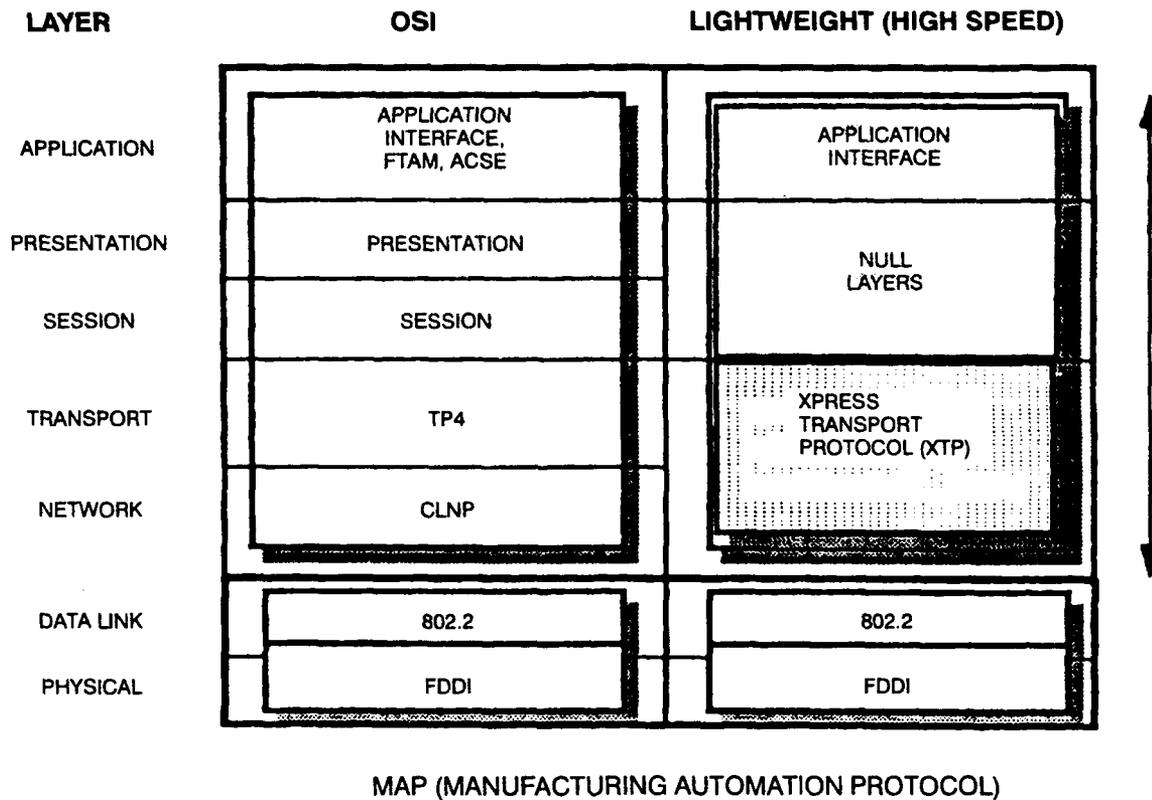


Figure 10. SAFENET profile.

The SAFENET physical topology consists of a dual Token-Ring network with a primary and secondary ring network at each installation. The components of the network are connected using Trunk Coupling Units (TCUs). The Dual Attachment Stations (DASs) that connect to the networks use fiber-optic interface connectors (FOICs) to send and receive fiber-optic signals.

The dual counter-rotating ring topology in SAFENET (see figure 11) is a major survivability feature of the standard. SAFENET networks automatically reconfigure in the case of a break or fault in one ring. Switching capabilities provide true transmission path redundancy.

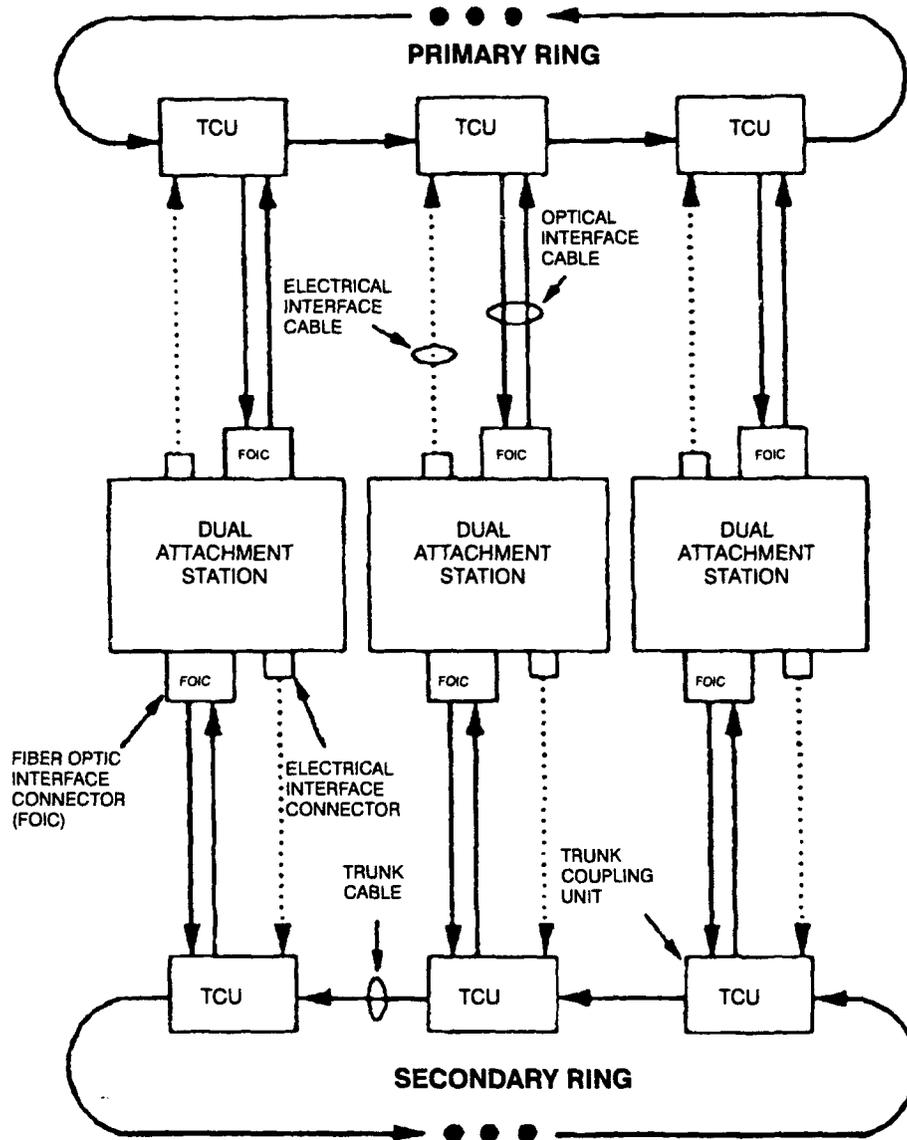


Figure 11. SAFENET topology.

WHERE IS LAN TECHNOLOGY HEADED?

LAN technology, like computer technology in general, is becoming faster, less expensive, and more reliable. Ethernet is the most widely used LAN technology. However, many network applications are constrained by Ethernet's maximum transfer rate of 10 million bits per second (Mbps). As shown in figure 12, this 10 Mbps, in real-world applications, yields a typical information transfer rate of 1 to 3 Mbps at the application level.

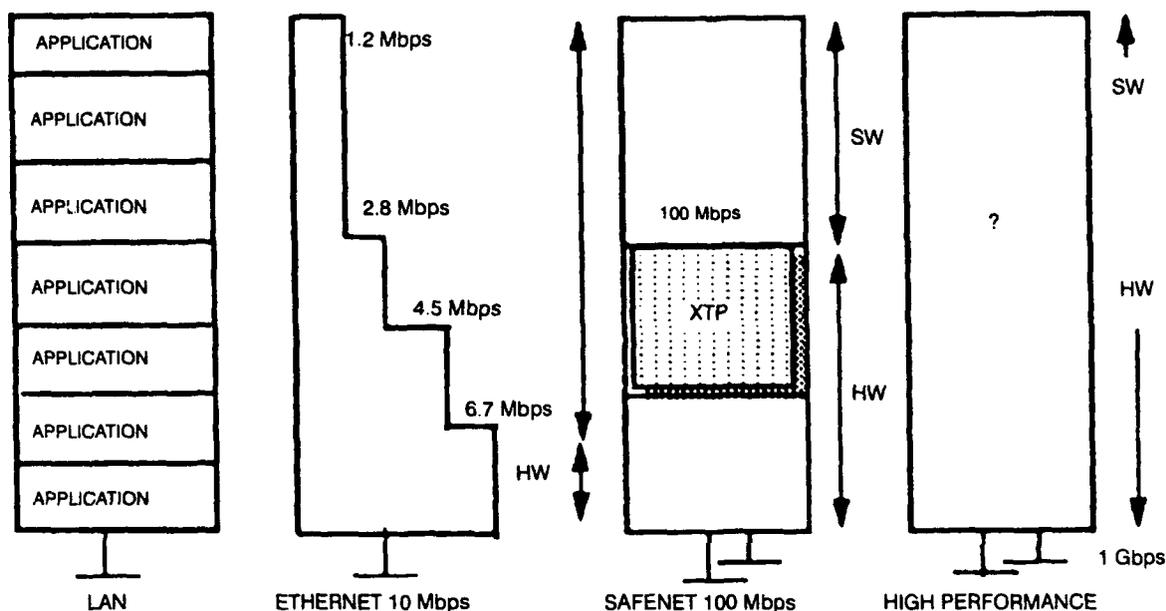


Figure 12. LAN technology trends.

New generations of computers demand much higher bandwidth to move larger amounts of information between processors. Processor performance on Reduced Instruction Set Computer (RISC) and Complex Instruction Set Computer (CISC) based systems has been doubling almost every 2 years. In 1985, a desktop computer with a rated performance of one million instructions per second (MIPS) was almost unheard of. At this point in history, a one MIPS machine is considered painfully slow.

New approaches to LAN communications are emerging and making use of new communications technologies such as fiber optics. Emerging LANs are performing in the Gigabit-per-second (Gbps) range and beyond. Throughput is being increased through the implementation of networking functions in hardware. An example of this is the implementation of the Xpress Transfer Protocol in SAFENET. FDDI (Fiber Distributed Data Interface) and ATM (Asynchronous Transmission Mode) are among the front-running proposals currently offered as advanced, high-performance LAN technology standards.

CONCLUSION

Open standards for networking have already been implemented in the form of the Internet network and have been resoundingly successful in the linking of tens of thousands of computers together. OSI is now providing a new set of worldwide standards for more complete, internationally accepted networking functions. SAFENET is a good example of a practical OSI implementation that provides Navy shipboard users with a much higher degree of performance, survivability, and flexibility in applying their processing resources.

REFERENCES

1. Boland, T. 1989. *Government Open Systems Interconnection Profile Users Guide*, National Computer Systems Laboratory, Gaithersburg, MD.
2. Bartee, T. C. 1986. *Digital Communications*, Howard W. Sams & Co., Indianapolis, IN.
3. Paige, J. L. and E. A. Howard. 1990. "SAFENET II—The Navy's FDDI-based Computer Network Standard," *FDDI, Campus-Wide, and Metropolitan Area Networks*, Proceedings, SPIE—The International Society for Optical Engineering, 19–21 September, pp. 7–13.

BIBLIOGRAPHY

- Andrews, W. 1992. "High-performance Networks Challenge Ethernet," *Computer Design*, (July) pp. 77–92.
- MIL-HDBK-0034. 1989. *Survivable Adaptable Fiber-Optic Embedded Network I*, (20 July) NOSC, San Diego, CA.
- MIL-HDBK-0036. 1991. *Survivable Adaptable Fiber-Optic Embedded Network II*, (15 January) NOSC, San Diego, CA.
- Rose, M. T. 1990. *The Open Book*, Prentice-Hall, Englewood Cliffs, NJ.

GLOSSARY

ACSE	Association Control Service Element, OSI layer 7 support package
ANSI	American National Standards Institute
Application Layer	OSI layer 7, exchanges information between application processes; examples are mail, EDI
ARPANET	Advanced Research Projects Agency Network, now divided into DDN, MILNET, and the INTERNET
ATM	Asynchronous Transmission Mode
BSI	British Standards Institute
CCITT	Consultative Committee for International Telephone and Telegraph
CISC	Complex Instruction Set Computer
CONP	Connection-Oriented Network Protocol
CLNP	Connectionless Mode Network Protocol
DARPA	DoD Advanced Research Projects Agency (now ARPA)
DAS	Dual Attachment Station
Data Link Layer	OSI Layer 2, transfers data over a single link
DDN	Defense Data Network
DECNET	Digital Equipment Corporation Network
DoD	Department of Defense
ECMA	European Computer Manufacturers Association
EDI	Electronic Data Interchange
FDDI	Fiber Distribution Data Interface
FIPS	Federal Information Processing Standard
FOIC	Fiber-Optic Interface Connector
FTAM	File Transfer, Access and Management Protocol
Gbps	Gigabits per second (billions)
GOSIP	U.S. Government Open Systems Interconnection Profile
HW	Hardware
IEEE	Institute of Electrical and Electronic Engineers
INTERNET	Formerly known as ARPANET
IP	Internet Protocol, Network layer protocol
ISDN	Integrated Service Digital Network
ISO/IEC	International Standards Organization International Electrotechnical Committee
ISO Protocols	A synonym for OSI Protocols

LAN	Local Area Network
LLC	Logical Link Control, part of layer 2, IEEE 802.2
MAC	Media Access Control, part of layer 2
MAN	Metropolitan Area Network
MAP	Manufacturing Automation Protocol
Mbps	Megabits per second (millions)
MCCR	Mission-Critical Computing Resource
MHS	Mail Handling System
MILNET	Military Network
MIPS	Million instructions per second
Network Layer	OSI layer 3, routing and relaying of data, end-to-end
NGCR	Navy's Next-Generation Computing Resources program
NIST	National Institute of Standards and Technology (formerly the National Bureau of Standards)
ODA	Office Document Architecture, layer 7 package
Open Systems Architecture	Specification of a set of nonproprietary international standards that allow, but does not insure, interoperability among a selected set of functional elements
OSI	Open System Interconnection, a set of nonproprietary international standards that specify open interconnection among computer systems
Presentation Layer	OSI layer 6, representation of information while in transit between applications
RISC	Reduced Instruction Set Computer
SAFENET	Survivable, Adaptable, Fiber optic Embedded Network
Session Layer	OSI layer 5, organize and synchronize the dialogues between application processes
SLWP	SAFENET Lightweight Protocol for layers 3 and 4
SNA	Systems Network Architecture
SW	Software
TCP	Transmission Control Protocol, transport layer protocol for INTERNET
TCP/IP	Set of INTERNET protocols developed by DoD ARPANET/MILNET/DDN networks
TCU	trunk coupling unit
TELNET	The application process offering virtual terminal service for INTERNET
TOP	ISO Technical Office Protocol

TP 0, 1, 2, 3	OSI Transport layer protocols for connection-oriented transport services
TP 4 Transport Layer	OSI Transport layer protocol OSI layer 4, packages and transfer data between end systems
Virtual Terminal	The OSI service to support a generic line-oriented terminal
WAN	Wide Area Network
XTP	Xpress Transfer Protocol, high-speed protocol for OSI layers 3 and 4 for SAFENET
X.25	OSI layers 1,2,3 protocols for using public-switched networks

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE <p style="text-align: center;">August 1993</p>		3. REPORT TYPE AND DATES COVERED <p style="text-align: center;">Final: January 1993</p>	
4. TITLE AND SUBTITLE <p style="text-align: center;">UNDERSTANDING OPEN SYSTEMS INTERCONNECTION (OSI)</p>			5. FUNDING NUMBERS <p style="text-align: center;">PE: 0602234N PROJ: 41-EC06-01 SUBPROJ: RS34P13 ACC: DN301142</p>		
6. AUTHOR(S) <p style="text-align: center;">G. B. Myers</p>			8. PERFORMING ORGANIZATION REPORT NUMBER <p style="text-align: center;">TD 2499</p>		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <p style="text-align: center;">Naval Command, Control and Ocean Surveillance Center (NCCOSC) RDT&E Division San Diego, CA 92152-5001</p>			10. SPONSORING/MONITORING AGENCY REPORT NUMBER		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) <p style="text-align: center;">Naval Command, Control and Ocean Surveillance Center (NCCOSC) RDT&E Division San Diego, CA 92152-5001</p>			11. SUPPLEMENTARY NOTES		
12a. DISTRIBUTION/AVAILABILITY STATEMENT <p style="text-align: center;">Approved for public release; distribution is unlimited.</p>			12b. DISTRIBUTION CODE		
13. ABSTRACT (Maximum 200 words) <p style="text-align: center;">This document will serve as a guide for people who are new to the Open Systems Interconnection (OSI) concept. Described are concepts and defined are terminology important to achieving a better understanding of OSI.</p>					
14. SUBJECT TERMS <p style="text-align: center;">OSI; Survivable, Adaptable, Fiber-Optic Embedded Network (SAFENET); U.S. Government Open Systems Interconnection Profile (GOSIP); local area network (LAN); protocols; standards</p>				15. NUMBER OF PAGES <p style="text-align: center;">26</p>	
17. SECURITY CLASSIFICATION OF REPORT <p style="text-align: center;">UNCLASSIFIED</p>				16. PRICE CODE	
18. SECURITY CLASSIFICATION OF THIS PAGE <p style="text-align: center;">UNCLASSIFIED</p>		19. SECURITY CLASSIFICATION OF ABSTRACT <p style="text-align: center;">UNCLASSIFIED</p>		20. LIMITATION OF ABSTRACT <p style="text-align: center;">SAME AS REPORT</p>	

UNCLASSIFIED

21a. NAME OF RESPONSIBLE INDIVIDUAL Dr. G. B. Myers, Jr.	21b. TELEPHONE (include Area Code) (619) 553-4136	21c. OFFICE SYMBOL Code 4102

INITIAL DISTRIBUTION (U)

Code 0012	Patent Counsel	(1)
Code 02712	Archive/Stock	(6)
Code 0274B	Library	(2)
Code 40	R. C. Kolb	(1)
Code 41	R. B. Volker	(1)
Code 4102	G. B. Myers, Jr.	(20)

Defense Technical Information Center
Alexandria, VA 22304-6145 (2)

Navy Acquisition, Research & Development
Information Center (NARDIC)
Arlington, VA 22244-5114

Center for Naval Analyses
Alexandria, VA 22302-0268

NCCOSC Washington Liaison Office
Washington, DC 20363-5100

GIDEP Operations Center
Corona, CA 91718-8000

NCCOSC Division Detachment
Warminster, PA 18974-5000