NIST Special Publication 500-192

Computer Systems Technology

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology

Government Open Systems Interconnection Profile Users' Guide, Version 2

Tim Boland

NIST Special Publication 500-192

Government Open Systems Interconnection Profile Users' Guide, Version 2

Tim Boland

Computer Systems Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899

Supersedes NIST Special Publication 500-163

October 1991

U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary
NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
John W. Lyons, Director

Reports on Computer Systems Technology

The National Institute of Standards and Technology (NIST) has a unique responsibility for computer systems technology within the Federal government. NIST's Computer Systems Laboratory (CSL) develops standards and guidelines, provides technical assistance, and conducts research for computers and related telecommunications systems to achieve more effective utilization of Federal information technology resources. CSL's responsibilities include development of technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive unclassified information processed in Federal computers. CSL assists agencies in developing security plans and in improving computer security awareness training. This Special Publication 500 series reports CSL research and guidelines to Federal agencies as well as to organizations in industry, government, and academia.

National Institute of Standards and Technology Special Publication 500-192
Natl. Inst. Stand. Technol. Spec. Publ. 500-192, 166 pages (Oct. 1991)
CODEN: NSPUE2

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1991

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

FOREWORD

This GOSIP Users' Guide, a companion to the GOSIP Version 2.0 FIPS 146-1, supersedes NIST Special Publication (SP) 500-163, which was issued in August 1989. Material in this revised document which was not in the previously-referenced document includes the following: Virtual Terminal, ISDN (Integrated Services Digital Network), Connection-Oriented Network Service (optional), Connectionless Transport (optional), and the end system to intermediate system (ES-IS) routing protocol. Major new material is also given on GOSIP registration procedures. These changes are the result of additions of functionality in the GOSIP Version 2.0 FIPS 146-1, as well as errata due to greater experience.

1.0 INTRODUCTION

1.1 Welcome

Welcome to the world of the Government Open Systems Interconnection Profile (GOSIP). Open Systems Interconnection (OSI) is a revolutionary concept in data communications whereby computer systems are able to communicate in an open environment without knowledge of specific characteristics of remote host computers. The OSI approach makes possible a wide degree of interoperability between a variety of computers manufactured by different vendors.

The benefits of OSI for the U.S. Government are (1) effective, interoperable networking solutions saving money and providing increased communications capability, (2) minimal additional networking related software development costs, and (3) competitive products marketed on a worldwide basis by U.S. computer vendors. These benefits may be realized via GOSIP [NIST 2]; both GOSIP and OSI will be explained in this document. Unless specifically stated otherwise, references to GOSIP in this document will be to GOSIP Version 2.

OSI concepts are expected to drastically alter the Federal workplace for the user in the 1990s. These concepts satisfy a need that has been perceived since the early 1970s, when it was recognized that a lack of interoperability among heterogeneous computer systems would not be of benefit to U.S. Government integrated applications in the near future. The progression of the OSI effort is as follows: (1) development of international standards, (2) vendor and user agreements based upon these standards, (3) development of OSI communications products based upon these standards and agreements, and (4) development of tests for products showing conformance to the standards and demonstrating interoperability between products.

The importance of OSI concepts is manifest in the trend toward smaller, less expensive, and more powerful computer systems in today's world. Federal agencies are able to benefit greatly from OSI technology; GOSIP is a technical specification which gives detail necessary for Federal agencies to purchase OSI-based products and use them effectively.

Even though GOSIP provides essential information to benefit U.S. Government users, there is also additional information which needs to be provided to complete the GOSIP assimilation process. This GOSIP Users' Guide attempts to fill this gap in information and complete resolution of outstanding issues; it is meant to be a service and aid to the user.

1.2 Nature and Purpose of Guide

The expected audience for this Guide is: (1) Federal procurement specialists (or their agents), (2) Federal technical specialists, and (3) Federal managers and executives. By consulting this Users' Guide, Federal procurement personnel learn how to purchase GOSIP products, and Federal technical personnel learn how to evaluate those products for technical merit. Federal managers and executives, while interested in the technical issues, also learn how to develop project plans and goals around GOSIP by using this Guide.

This Guide consists of short, diverse sections, each designed to assist the U.S. Government user in understanding and interpreting GOSIP technical information, and to enable the user to assimilate GOSIP-compliant products into the workplace. Each section addresses a different topic. There are certain sections which everyone should read; other sections may be read selectively (or in part).

For example, the Federal procurement official needs to be aware of acquisition requirements for GOSIP-compliant products. The Federal technical expert needs to be acquainted with technical details relating to the installation, maintenance, operation, and evaluation of OSI products. The manager needs to plan and develop life cycle system strategies for reducing costs and increasing application effectiveness.

This Users' Guide is designed for the individual who has little or no experience in OSI implementations. Anyone with no previous exposure to OSI should be able to read and understand all portions of this Guide;

however, the individual who has some experience in OSI may also gain insight from this Guide.

This Users' Guide serves as a companion document to Version 2 of GOSIP, issued as Federal Information Processing Standard (FIPS) 146-1, and is best used in conjunction with GOSIP and/or OSI documents. This Guide progresses from a general outline of the subject to specific detail. Appendix D contains a form the reader may use to provide comments, questions, and suggestions for improving later versions of the Users' Guide. Such input is greatly encouraged and greatly appreciated.

1.3 Brief History of OSI

The concept of OSI (Open Systems Interconnection) was developed to enable heterogeneous computer systems to interoperate in a data communications environment. This means that users on one host can communicate with users on another host without specific knowledge of the characteristics of the other machine.

To reduce design complexity, the OSI architecture is organized as a series of layers or levels, each one built upon its predecessor. Specific communications functions are contained in each layer. The purpose of each layer is to offer certain services to the higher layers, shielding those layers from the details of how the offered services are actually implemented.

The N layer on one machine carries on a conversation with the N layer on another machine. The rules and conventions used in this conversation are collectively known as the N layer protocol. The entities composing the corresponding layers on different machines are called peer processes. In other words, it is the peer processes at the N layer that communicate using the N layer protocol. Figure 1 illustrates this scenario.

Some of the principles of the OSI Reference Model [ISO 1] are: (1) each layer performs a well-defined function, (2) minimal information flows across layer boundaries, and (3) internationally standardized protocols should be "derivable" from the functionality of each layer. The OSI Reference Model deals with communications functionality

There are seven layers in the OSI Reference Model. These layers are referenced in the GOSIP FIPS. They are the: (1) Physical Layer, (2) Data Link Layer, (3) Network Layer, (4) Transport Layer, (5) Session Layer, (6) Presentation Layer, and (7) Application Layer. Each layer has a protocol specification, or a set of rules governing dialogue between peer processes (processes at the same level), and a service definition, which describes an abstract interface to the next higher level. Each of the layers uses the service of the next lower layer; in turn each layer provides a service to the next higher layer (see fig. 2).

Layers 1 through 3 define machine-to-machine communication via intermediate systems. Layer 4 defines end-system to end system communication, and layers 5 through 7 address user-oriented functionality. The interface definitions and the protocol layer definitions indicate that each layer may be modified independently of the adjacent layer, and that processes at a certain layer need not have detailed knowledge of processes occurring at other layers. Many references are made to these concepts in the GOSIP FIPS; for additional information, readers may look in Appendix A of this Guide, which will give tutorial material on OSI. Specific publications referenced in Appendix B will also guide the reader on an introductory tour of OSI.

Though work remains to be done, detailed standards are now in place for the entire seven layers, and the focus is on developing products based on OSI that the user can use. In this regard, GOSIP was developed to enable the Government to take advantage of the emerging OSI technology.

Work done by implementor groups, such as the MAP/TOP group (see sec. 3) and the OSI Implementors Workshop (see sec. 3), serves to further define OSI in the context of specific systems and applications. Demonstration events which have taken place serve to highlight accomplishments and to provide a practical forum to illustrate the workability of OSI in a practical sense. The Enterprise Networking Event (ENE) in June 1988 was the first major OSI product exhibition. For additional material on the relationship between the OSI development process and GOSIP, refer to section 3 of this Guide.

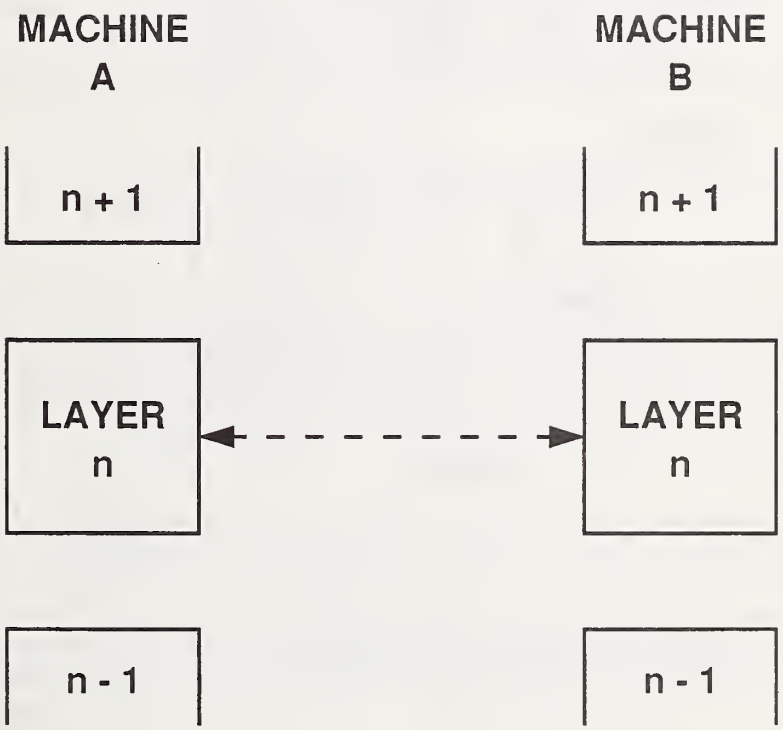


FIGURE 1
OSI COMMUNICATION

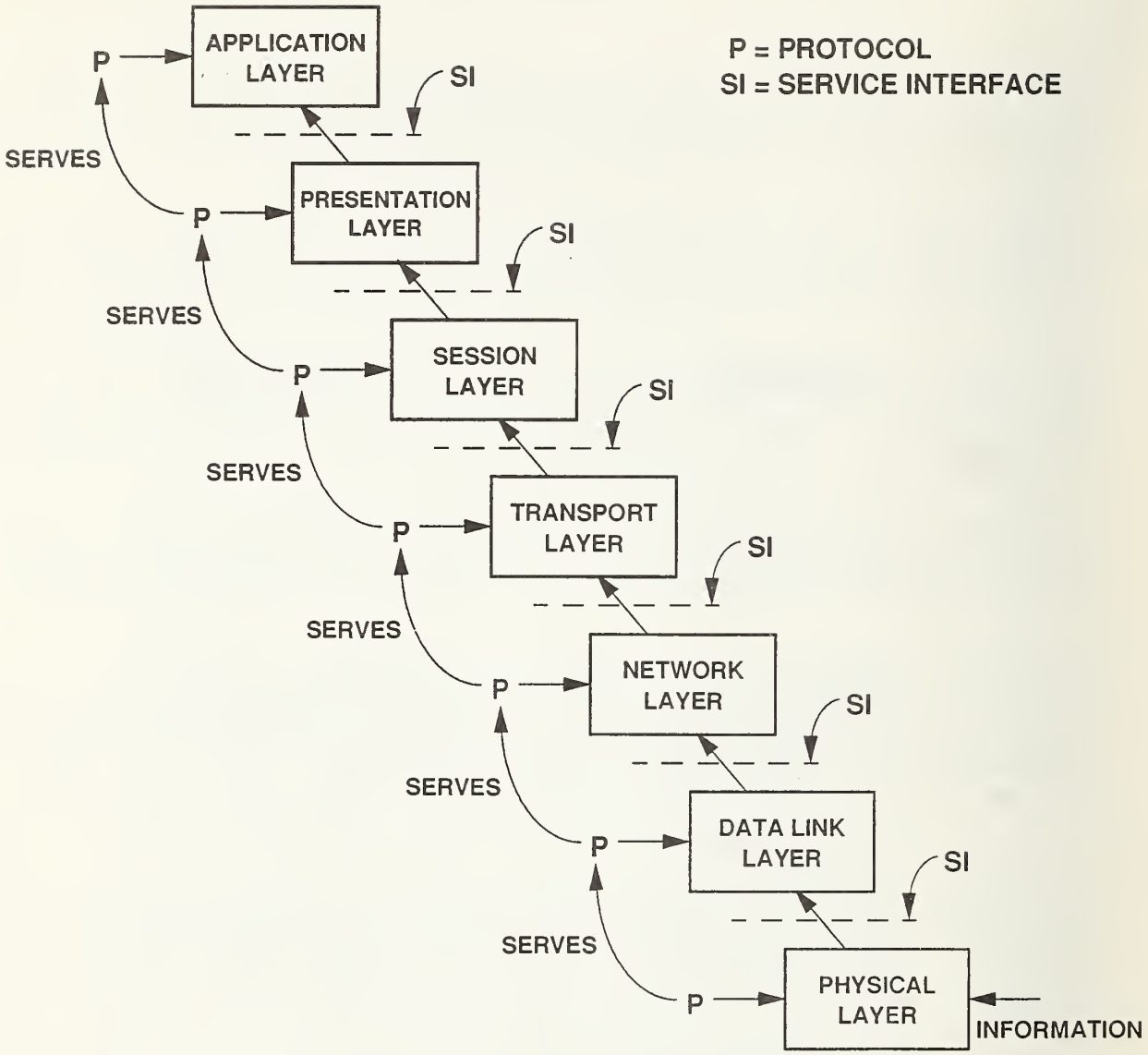


FIGURE 2
OSI LAYERING DEFINITION

1.4 Role of GOSIP

GOSIP is a result of a desire to simplify and ease the process of assimilating OSI technology into Federal agencies by: (1) specifying a common generic set of requirements (to avoid having users independently consult a plethora of complicated standards), and (2) ensuring stability in OSI material referenced in Federal procurement efforts. Version 2 of GOSIP is a technical specification which contains a core set of protocols and services; future versions of GOSIP will contain additional functionality. Version 1 of GOSIP, issued in August 1988, is, with the exception of some errata, subsumed into Version 2 of GOSIP.

A Federal agency may have hundreds of disparate information systems which are not interconnected and which include products from virtually every vendor. The resulting heterogeneous environment may exhibit a high degree of incompatibility in terms of hardware, software, data, and communications. This incompatibility may lead to problems such as inefficiency, poor performance, high expense, and a general feeling that things are out of control. It is problems such as these which GOSIP is designed to correct.

GOSIP defines and describes a common set of data communications protocols which enable systems developed by different vendors to interoperate and enable the users of different applications on these systems to exchange information. These protocols were developed by international standards organizations, primarily the International Organization for Standardization (ISO) and the Consultative Committee for International Telegraph and Telephone (CCITT). GOSIP is based on agreements reached by vendors and users of computer networks participating in the National Institute of Standards and Technology (NIST) Workshop for Implementors of Open Systems Interconnection.

GOSIP specifies a subset of OSI protocols, and may be described as a selection of a limited number of OSI protocols from each layer of the OSI Reference Model, as appropriate. Such selection is necessary for procurement reasons.

GOSIP is to be used by Federal Government agencies when acquiring computer network products and services and communications systems or services that provide equivalent functionality to the protocols defined in GOSIP documents. For the indefinite future, agencies will be permitted to buy network products in addition to those specified in GOSIP and its successor documents. Such products may include other non-proprietary protocols, proprietary protocols, and features and options of OSI protocols which are not included in GOSIP.

GOSIP Version 1 was mandatory in August 1990. GOSIP Version 2 supersedes GOSIP Version 1. Configuration issues and other issues in referencing GOSIP Version 2 will be addressed in this Guide.

The appendices to the GOSIP specification describe advanced requirements for which adequate profiles have not yet been developed. Federal government priorities for meeting these requirements and the expected dates that work on these priorities will be completed are also provided. More information on each of these subjects is given in section 7.

1.5 Format and Layout of Guide

Section 1 provides background and introductory material. Section 2 provides an overview of the benefits of OSI from different perspectives (economic, functional, and planning); this section should be read by those interested in the motivation for this effort.

Section 3 gives a perspective on how protocols mature and are included in GOSIP. The relationship of GOSIP to other OSI-based documents and how GOSIP advanced requirements will be included in future GOSIP releases is also specified.

Section 4 contains a list of commonly asked questions about the GOSIP FIPS, with corresponding answers. This is of benefit to users who desire a quick introduction to or a quick summary of GOSIP.

Section 5 gives a general statement of GOSIP applicability to Federal ADP environments. Also included is a description of the waiver management process, GOSIP enforcement issues, and additional recommendations and considerations for GOSIP applicability.

Section 6 gives information on strategies that agencies should use to procure GOSIP-compliant products and services. This section should be read by Federal procurement personnel.

Section 7 provides insight into technical aspects of OSI communications, assisting the proper evaluation of GOSIP products. This section should be read by technical personnel and managers, and provides supporting documentation for the procurement process elaborated in the previous section.

Section 8 describes objects which need to be registered, and gives instructions on how to register these objects. This section should be read by all system managers and technical managers. Future registration issues are also discussed.

Section 9 gives information on life-cycle management; this section includes recommendations for planning and executing generic transition strategies from proprietary systems to OSI-based systems. Some detailed case histories are given mentioning plans that may be used for particular situations.

Section 10 provides references on other programs which may interact with GOSIP systems in the near future (FTS2000, POSIX, CALS, EDI, GNMP, ODA, SGML, CGM). There are a variety of standardization activities taking place in the Federal sector in the near future, and it is important that managers and planners keep track of developments.

Appendix A gives detailed tutorial information on OSI and some important components (including File Transfer, Access and Management, Message Handling Systems, and Virtual Terminal Applications). Users desiring additional knowledge of OSI and related topics should read Appendix A. Appendix B gives points of contact and additional reference material for those wishing more information. Appendix C gives a list of participants in an important OSI-related activity (see sec. 3.2.2). Appendix D provides a form to be used for comments, questions, and suggestions.

In summary, procurement personnel should read sections 1, 5, 6, and 10; executives should read sections 1, 2, 4, and 10, and technical personnel should read sections 3, 7, 8, and 9. However, Federal agency personnel who need to know more about the GOSIP process and protocols are encouraged to read all sections of this Guide.

1.6 Acknowledgments

The author wishes to thank the personnel at the National Institute of Standards and Technology who assisted in the preparation of this Guide, including Jerry Mulvenna, Kevin Mills, Dale Walters, Doug Montgomery, Richard Colella, and Shirley Radack, among others. Other personnel from various Government agencies who have assisted in various portions of this Guide are: Bruce McLendon of NASA, Ray Denenberg of the Library of Congress, Jerry Cashin of the Air Force Computer Acquisition Center, Jerry Gibbon of the Department of Commerce, Robert Buckley of the Navy Deparment, and Leon Blue of the State of Florida, among others.

Persons assisting in the creation of this revised Users' Guide include: Bill Ohle of the General Services Administration, Charles Parisot (formerly of Boeing Computer Services), Raomal Perera and Tom Lane of Retix, and Cyndi Jung of 3COM. In particular, Raomal Perera and Tom Lane of Retix were instrumental in the preparation of the Virtual Terminal tutorial. Personnel from NIST who have similarly assisted include Roger Sies and Steve Trus.

2.0 OVERVIEW FOR EXECUTIVES

2.1 Introduction

GOSIP is expected to dramatically alter the way the Federal Government purchases ADP communications technology. In order for maximum benefit to be gained from this new technology, strategic planning initiatives should be developed now at the highest echelons of Government. In order for this to happen, Government executives must be informed of the long-term benefits of OSI technology, and be assured that this technology is relevant to their agency. Accordingly, benefits will be presented from planning, functionality, and economic perspectives. These benefits should convince Government executives that an OSI approach is the direction to take.

The benefits of standardization to the U.S. Government are many, for both the user and the vendor. Formerly, Federal agencies have been locked into the services provided by their current ADP vendors because existing systems will not interoperate with systems marketed by other vendors. Now, users may choose the best network solutions without being locked into a specific vendor. Small- to mid-sized vendors may effectively compete in the open marketplace. Also, in the modern world, there is an increasing need to share information, to communicate beyond the narrow confines of a particular organization. This communication is only possible if standard protocols are developed which allow systems built by different vendors to exchange information.

A wide variety of products that implement these protocols is available now. More products providing additional services will be available in the near future. This section introduces the Federal executive to the advantages of incorporating GOSIP-compliant systems into the Federal ADP environment.

GOSIP does not require Federal agencies to completely replace existing data communications software. It does require Federal users to procure OSI products when they are procuring the services which OSI products provide. This will ensure multi-vendor interoperability. Federal agencies may also procure non-OSI products with additional desired capabilities.

Imposition of GOSIP will encourage competitive procurements and facilitate development of centralized agency policies relating to data communications procurement. A kernel set of capabilities exists in OSI products; this set will become much larger over time, promoting multi-vendor interoperability. OSI products are based upon technically stable standards and agreements (see sec. 3). Furthermore, a world market is being created for OSI products, so that vendors should be able to sell not only to the U.S. Government, but also to other users in America and around the world.

GOSIP allows users the ability to incorporate communications facilities in such a way as to promote interoperability and connectivity. The aim of OSI standards is to facilitate the accomplishment of user objectives through the incorporation of state-of-the-art communications technology. The level of commitment of agency resources to incorporate OSI products need not be large over the long term, and it is possible to move to the OSI environment with a minimum of disruption, as is being illustrated by the Department of Defense.

To the executive, this means that project plans may proceed along predictable lines; agency heads should be able to plan system upgrades with confidence. Manpower and human resources can be saved and program goals need not be sacrificed for computer and system limits. Agency heads can satisfy program objectives and be guaranteed support from data processing facilities. In short, adopting OSI as a strategic policy will ultimately lead to improved information transfer within an agency, with attendant benefits.

2.2 Economic Benefits

Projected cost savings over the life cycle of a computer or network system may be substantial when using GOSIP as contrasted with alternative choices; furthermore, the longer the life cycle, the greater the savings. This is due to several factors described below.

First, small- to mid-sized vendors can market OSI products competitively with larger vendors. Since more vendors can compete for a share of the market, total projected costs for the consumer should be reduced. As with any supply-and-demand situation, a larger number of vendors entering the market means the price for the customer may be minimized, because of the increased competition. The larger the number of vendors entering the competitive procurement process, the lower the final prices are likely to be.

The second factor is implementation variety. GOSIP-compliant products are expected to be offered and designed to vary in price. Increased competition and resultant lowered final prices may enable customers to choose the best network solution based upon user needs.

The third factor keeping prices down is the avoidance of excessive software development costs. The cost of hardware in general is expected to remain fairly stable over time; software costs are expected to continue to rise dramatically over the next several years. Software development is a "human intensive" effort requiring large numbers of people as well as training and management expertise. The implementation of GOSIP tends to reduce these costs. Communications software development is minimized because GOSIP relies on an open communications architecture, whereby machines are able to interoperate without need for special purpose software to connect each machine to each of the other machines on the network.

The fourth major factor keeping costs down is that interoperability of aging OSI equipment with evolving OSI equipment is possible when following GOSIP; thus, an agency is able to avoid expensive purchases of computer equipment in the future to achieve a certain level of communications functionality and interoperability. Users may cost effectively switch to lower-cost or higher-performance vendors without losing GOSIP interoperability.

The final major factor is that establishment of a standard architecture like that referenced in GOSIP allows a hardware base upgrade without losing the investment in software. A customer is able to add new hardware components to existing systems without the requirement to purchase expensive new software. A GOSIP-compliant solution for interoperability is likely to be less expensive than a special custom-designed solution for a particular configuration.

Some other cost saving factors of OSI products must be mentioned as well. The modular approach to OSI design enables modifications to be made more efficiently. Also, once an initial OSI training period is past, future training and overhead costs should be relatively low.

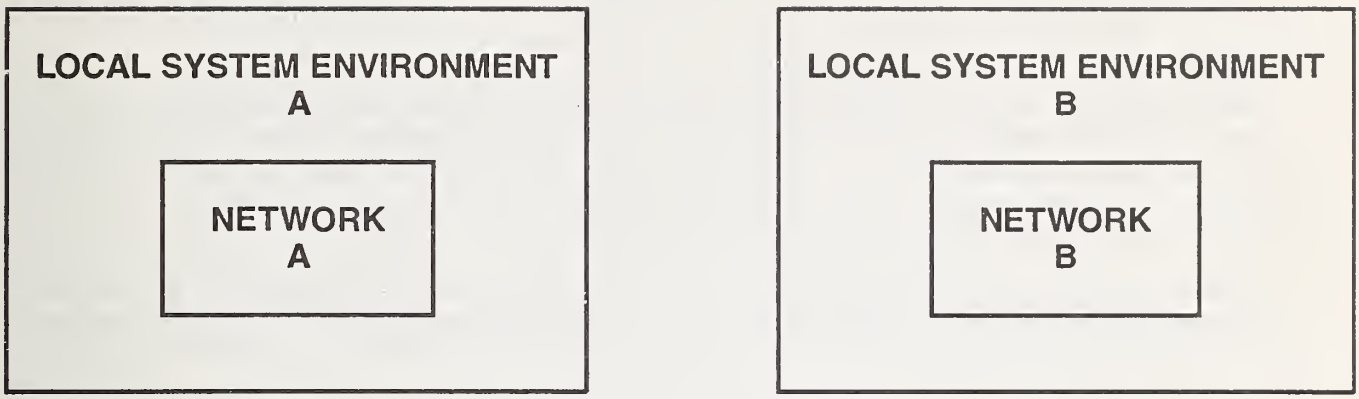
In sum, acceptance of OSI technology offers substantial cost savings that should grow over the life cycle of the system. Furthermore, these savings are largely predictable, in the sense that vendors are able to meet with an agency to develop long-term solutions which will minimize long-term costs.

2.3 Functional Benefits

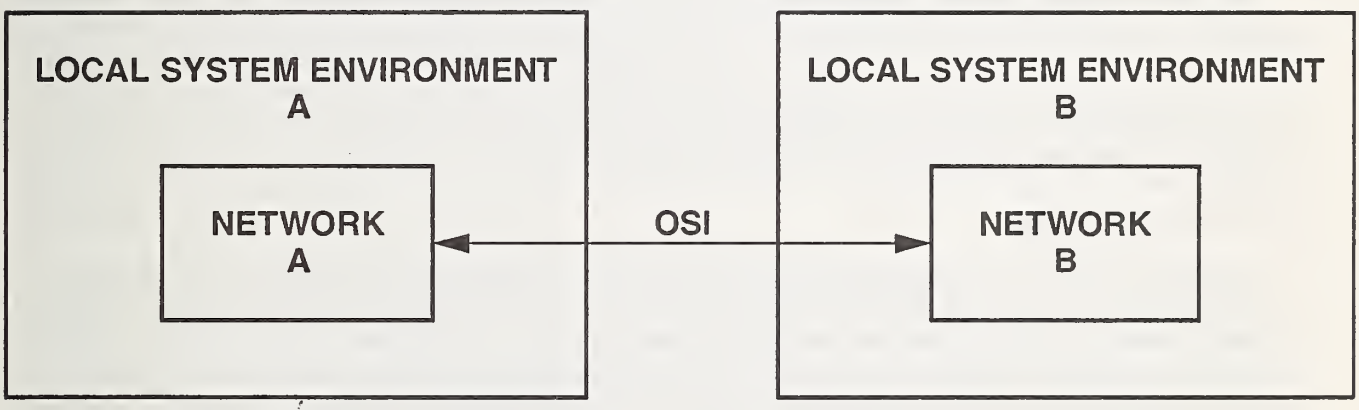
Functional benefits of OSI implementation are as follows: (1) interoperability without loss or compromise of local system environments (user interfaces), (2) enhanced services available with OSI applications, (3) a growth in capabilities over the next few years, (4) the selection of options and features that best satisfy a stated need, and (5) a reliable end-to-end transfer service over which standard and nonstandard applications may be written. Each of these benefits is explained in some detail below.

For (1), the adoption of a standard architectural solution for interoperable data transfer allows existing and future networks to be interconnected, thus enabling users on one network to communicate effectively with users on other networks. This can be accomplished without the need for a vendor to modify existing user interfaces, because there is no need to do so to achieve multi-vendor interoperability. Thus a vendor may add GOSIP-related services while preserving special end-user services. The above-described scenario is illustrated in figure 3. As as example, GOSIP electronic mail protocols may be used to interconnect existing electronic mail systems.

For (2), in general, GOSIP applications offer many services and features not found in many current



a) BEFORE



b) AFTER

FIGURE 3
INTERCONNECTION SCENARIO

products. The GOSIP electronic mail service gives users additional capabilities not found in many current mail systems. without losing capabilities found in these current systems. The GOSIP file transfer service and virtual terminal protocol give users many functional benefits not found in current file transfer systems and virtual terminal applications. Future GOSIP applications are expected to offer similarly enhanced capabilities over current systems in the appropriate functional areas.

For (3), GOSIP Version 1 provided the foundation upon which to add new protocols providing new services. Version 1 of GOSIP provides for the reliable transfer of data between end systems of different types of networks, as well as electronic mail and file transfer applications which use this reliable transfer service. Version 2 of GOSIP builds upon that foundation by adding the virtual terminal service application and by adding ISDN as a network technology supporting OSI applications.

For (4), multi-vendor competition means that a user can differentiate and choose OSI products based on specific features and options that best satisfy a user's functional requirements; thus, a product can be custom-designed to satisfy particular user wishes while satisfying GOSIP requirements. Furthermore, the OSI architecture allows for options that may be used in this way.

For (5), GOSIP provides for a reliable end-to-end transfer capability. This capability is able to support many different applications and user environments. Users may write or buy their own applications to exploit this capability.

In sum, the increased scope of existing applications and network configurations and the increased power of these same applications and configurations can allow more productive work to be accomplished in a shorter period of time. A number of capabilities are expected to be provided in OSI products that have not been provided previously. In addition, current OSI capabilities are state-of-the-art, and represent the latest advances in networking technology. GOSIP is bringing up-to-date communications knowledge, technology, and products to Federal agencies.

2.4 Planning Benefits

There are a number of administrative and planning benefits available to executives when OSI technology is implemented, and when a GOSIP direction is set. The emergence of GOSIP means that agencies should be able to predict networking expenses in the future for procurement, upgrades, manpower, future resource allocations, and future capabilities. This is because the OSI concept allows for a steady development and progression of capability which is based upon backward compatibility and widening interoperability. An agency may add resources and capability gradually, or rapidly, depending on preference. Throughout the life cycle of a system, the need for unexpected, large purchases should be diminished.

The increased interoperability possible with OSI products means that diverse networks are connected, and different centers of network control and management may be consolidated into one level of control. This should allow for simplified configuration management, and much simpler control planning. Agency-wide policies may be set up governing computer use, and computer resources across an agency can be managed from a central location. Paperwork and human resources can be reduced. Again, a single policy can be established for an agency covering communications, and can remain in force for the indefinite future. Control over networking capabilities can be exercised from a single point. It should be easier to plan long-term ADP procurements.

Finally, adoption of GOSIP allows agencies, to a greater extent, to develop policies that are independent of any particular ADP environment. Agency programs should serve the user, based upon the user's stated needs; the use of GOSIP in procurement can enable those needs to be more directly met. More attention from a planning perspective may be paid to what service an agency is providing according to its mission, and not to the complex details of how that agency operates in meeting its commitments from a computer-related standpoint.

In sum, the adoption of GOSIP means that agencies can have a much greater degree of control over

long-term planning. Cost and resource projections may be given far into the future with confidence. This can increase overall agency efficiency, and allow an agency to concentrate to a greater extent on long-term program priorities, rather than on communications capability.

2.5 Summary and Direction

A comprehensive set of benefits to be gained by using OSI technology was explained above. It should be apparent at this point that adopting OSI as the key data communications strategy now and in the future is a wise idea. Such adoption can assist agencies in meeting their program goals now and in the future more efficiently and less expensively than would otherwise be possible.

In light of the above discussion, what is the next step for an agency executive? The answer is that a comprehensive strategic initiative should be developed at the highest levels of an agency at the earliest possible time. If possible, such a strategy embracing the OSI concept should be formally adopted as specific agency policy. The U.S. Congress, the Office of Management and Budget, the Department of Commerce, and the Department of Defense (DOD) have all endorsed the concept of OSI and GOSIP.

A long-term commitment should be made by agency executives to support GOSIP in all future networking decisions. This commitment should be clear and unambiguous, and should have the support of the highest ranking officer of an agency as a public declaration. Once a future networking decision based on OSI is set, vendors should be notified, specific transition plans should be developed, and orderly integration of OSI products into the appropriate Federal work environments can begin. The DOD and the Department of Energy have already endorsed GOSIP at the policy level, and have issued an OSI implementation plan. NASA (National Aeronautics and Space Administration), and the Department of the Interior, among others, are similarly defining implementation strategies for GOSIP.

Other industry groups, such as the AIA (Aerospace Industries Association), are investigating the feasibility of GOSIP for their needs. State governments, including those of Florida, Minnesota, and Oregon, are looking to adopt GOSIP solutions to their interoperability concerns. Countries around the world are looking to OSI for long-term solutions (see sec. 3.5).

In summary, an agency executive should examine specific programs, organizations, and goals within the agency to determine how the benefits of GOSIP can best be realized. A clear focus should be established; the question "What should the status be of agency communications at a specified point in the future?" should be answered. Appropriate support personnel should be consulted in this regard. Other sections of this Guide give specific assistance in moving forward toward OSI integration once a definite policy is in place.

3.0 PERSPECTIVE ON GOSIP

3.1 Introduction

This section gives a perspective on the GOSIP process. The benefits of OSI are numerous, as previously described. The promulgation of GOSIP as a FIPS represents a major accomplishment in bringing OSI technology into the Federal workplace. A number of steps were necessary to reach this advanced point, and they are described below.

The inclusion of specific OSI communication protocols and services into GOSIP is no accident. There is a deliberate, organized process by which this work matures and becomes useful. The pace of development of OSI work may seem relatively slow, but this is to ensure that the work in place is stable. There is another time factor at work, however, as reflected in the desire for users to see marketable OSI products as soon as possible. The creation of a user market drives the vendors and gives impetus to the OSI development effort. In turn, the vendor must be convinced that users will buy OSI products; thus, vendors and users continue to give impetus to each other in the push for worldwide interoperability.

There are several characteristics common to all of the protocols referenced in GOSIP. These are: (1) wide applicability (generally useful not only to U.S. agencies, but on a worldwide basis), (2) availability (implementations exist now or will be available in the near future), (3) stability (protocols are technically "frozen" and are not expected to change in the foreseeable future), and (4) effectiveness (the protocols will solve a common need of the Federal agencies). In addition, vendors and users alike must agree on marketing and transition strategies to integrate this technology into the workplace. This process is occurring now in many installations.

3.2 Steps to GOSIP

Below are given some of the critical steps in OSI development, from recognition of need to development of an environment in which GOSIP was created.

3.2.1 Standards Development

The beginning of the process is the recognition of deficiencies in some aspect of communications. For example, file formats and structures on dissimilar systems may be completely incompatible, but may need to be integrated in one large application. The overall lack of interoperable configurations is a general problem, emphasized previously in this document.

In the early 1970s, as knowledge of computer networking increased, the potential and problems in its use became apparent. By the late 1970s, lack of interoperability and lack of compatibility between different machines posed significant problems in data communications. Users were "locked" into specific vendor solutions, local software development costs were high, small vendors could not market products competitively worldwide, and so on. In order to interoperate in the 1970s, a specialized interface had to be developed between any two machines; as the number of machines grew, so did the number of required interfaces, to an unacceptable level.

This is the general problem. To solve this problem, the Defense Advanced Research Projects Agency (DARPA) of the Department of Defense (DOD) developed a nonproprietary set of protocols that would allow different machines to communicate more efficiently and effectively. The DARPA protocols [DOD 1-2] represented a major advance in this direction, and the DARPA protocols were mandated in 1982 for DOD-wide use. A National Research Council (NRC) study [MISC 3] has recommended that the DOD evolve to use OSI protocols, and the DOD has subsequently endorsed the OSI concept [DOD 3].

In the late 1970s, the International Standards Organization (ISO) (now the ISO/IEC) developed a common reference model which partitioned the functions involved in data communications into seven layers. Committees and subcommittees were formed, and the work of developing standards for the seven layers

began. Vendors and users provided input into the process, based upon real-life experiences and concerns. These meetings were (and are) open to all interested participants.

Independently of the ISO, the Consultative Committee for International Telegraph and Telephone (CCITT) began work on telecommunications-based interoperability standards. Due to the need for commonly defined and supported telecommunications-based capabilities, work progressed rapidly toward a set of agreements also based on the OSI architecture.

In 1979 the National Bureau of Standards (NBS) (now the National Institute of Standards and Technology (NIST)) initiated a program to support creation of standards that would meet U.S. Government needs for interoperable data communication. Since then, the NIST has actively encouraged and promoted the interests of Federal users in the ISO and CCITT standards development effort, and the resulting standards reveal this influence. The process desribed below is preserved in standards development today.

The early work of the ISO and CCITT produced "rough" documents which are still somewhat technically unstable. Member bodies of the organizations improve these documents by successive cycles of comment, input, and review; along the way, new drafts are created, and are fed back into the process.

The result of this process is a stable document, which (in the ISO/IEC) is an International Standard (IS); in the CCITT, this document is a CCITT Recommendation. In the ISO/IEC, the progression is: Working Draft, Committee Draft, Draft International Standard, and International Standard. In the CCITT this progression involves a 4-year program of work leading to a Recommendation. Member bodies in the United States are the American National Standards Institute (ANSI) for the ISO, and the Department of State for the CCITT. Figure 4 illustrates this arrangement.

In sum, key aspects of early standardization were: (1) the pioneering work of the DOD, (2) the telecommunications-based standards of the CCITT, and (3) the network-based standards of the ISO. The iterative processes described above continue today in further standardization. A "defect report" mechanism ensures high quality in existing ISO/IEC standards.

At first the most immediate problems involving OSI "lower layer" technology (see sec. 7) were investigated. This is because it is important to specify error-free transmission before specifying user-oriented applications relying on such capabilities.

In the past several years stable standards have been completed (in both the ISO and the CCITT) for a "full" seven-layer OSI "stack." This was a necessary step in the development of OSI products. A list of these standards is given in Appendix B.

Work is now underway on additional standards such as network management and security. These are important additional services to be included in OSI products. Work is also underway on addenda to existing standards to improve their functional capability. Finally, additional applications are being standardized; these applications include transaction processing and remote database access. It is a design goal that this new work be built on the previous work, so that OSI products may be "upwardly compatible."

It is important to remember that whenever possible GOSIP is based upon stable international standards. Sometimes, it may be necessary to reference work in GOSIP that is not based upon stable standards. If this happens, it should be viewed as an attempt to develop an interim solution to a critical user requirement.

3.2.2 OSI Implementors' Workshops

Generic standards by themselves are not sufficient to specify OSI product capabilities. Such standards include a number of options, subsets, and unspecified implementation details. In order to specify the necessary additional detail, after the standards have been completed, vendors and users have convened at locations around the world in a series of OSI implementors' workshops.

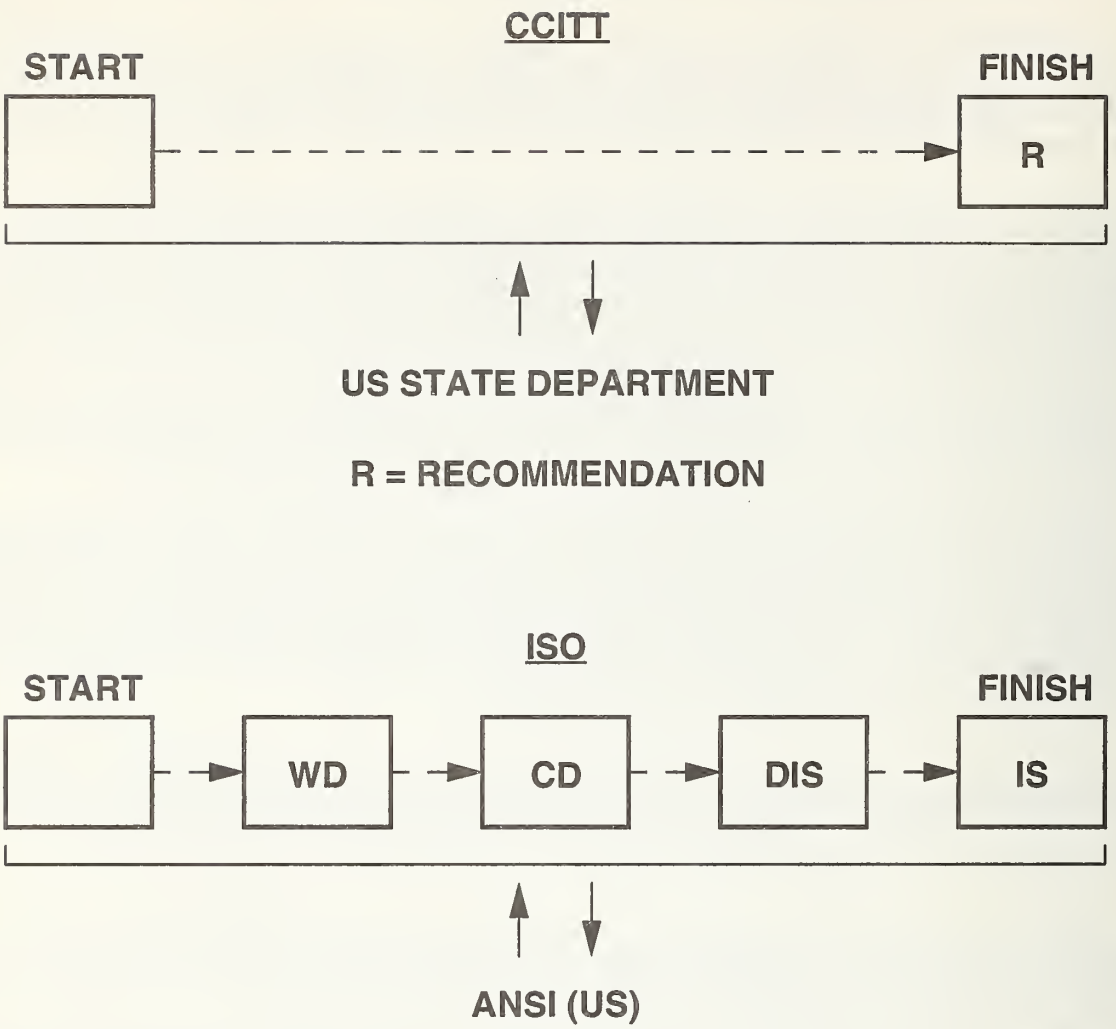


FIGURE 4
STANDARDIZATION PROGRESSION

The most prominent of these workshops is the OSI Implementors Workshop, held in Gaithersburg, Maryland, at the National Institute of Standards and Technology (NIST). This workshop is held four times per year to enable vendors and users to reach detailed agreements on OSI implementation issues. This workshop has been in existence since February 1983, and is administered by NIST. These meetings are open to all interested participants. GOSIP is based upon agreements reached at these meetings, in addition to being based upon the OSI standards themselves. This workshop is currently co-sponsored by the IEEE (Institute of Electrical and Electronics Engineers) Computer Society.

All organizations that encourage the development of OSI standards and that plan to implement or buy OSI systems are invited to participate in the workshop. The workshop is an established and effective mechanism for developing implementation agreements based on international OSI standards. The workshop is an open international forum, with participation of more than 200 computer manufacturers, semiconductor manufacturers, word processing vendors, process control vendors, communication carriers, and industry and government users from the United States, Canada, Europe, Australia, and elsewhere. The ultimate goal of the workshop is to promote OSI-based interoperability in multi-vendor environments. The workshop is also sensitive to testing concerns (see sec. 6.6).

Some typical computer and communications vendors participating in the workshop are: AT&T, Digital Equipment, Hewlett-Packard, IBM, and Unisys. Some prominent users participating in the workshop are Boeing, Department of Defense, General Motors, and the Veterans' Administration. For an expanded list of participating users and vendors, see Appendix C.

Documents of importance produced by the workshop are : (1) Stable Implementation Agreements for OSI Protocols (Stable Document), which gives implementor agreements that are not technically changing (except for errata), (2) Working Implementation Agreements for OSI Protocols (Working Document) which gives agreements that may be subject to technical change, and (3) the Workshop Procedures Manual, which governs the operation and conduct of the workshop meetings. In addition, there is a Style Manual. Release of a new version of the Stable Implementation Agreements for OSI Protocols ((1) above) occurs no more often than once per year.

All material in the Stable Document has been considered extensively in a review process, and has appeared in the Working Document for at least one Workshop period. The term "stable" in the context of the Stable Document means that (1) the material is not likely to change in the foreseeable future, and (2) the material may be referenced in procurement requests and test specifications.

The Working and Stable Documents are aligned and have a common structure. Material is either in the Working Document or in the Stable Document, but not both at once. Cross-references are made between the two documents, so that an implementor can take both documents together and determine what is stable, and what is non-stable (working) text.

Replacement pages, issued as appropriate after each workshop and reflecting technical, editorial, and alignment errata, are inserted into the latest version of the Stable Document. Technical errata alter the meaning of a piece of text, alignment errata are made in response to evolving base standards or profiles, and editorial changes are cosmetic in nature. New functionality may also be included as replacement pages. In this manner the latest version is maintained. Errata may also apply to previous versions of the Stable Document.

There are five important features of the workshop agreements. The first is that agreements are based upon stable ISO/IEC, CCITT, and other internationally recognized standards work as described in section 3.2.1. The second feature is that it is a goal for agreements to be "upwardly compatible"; that is, OSI products produced from one version will be able to interoperate correctly with OSI products from succeeding versions at the intersection of their capabilities. The third feature is that international harmonization and alignment efforts are underway with similar groups in other regions, with the goal of creating compatible worldwide implementation specifications. There is a Regional Workshop Coordination Committee (RWS-CC) which is

chartered with the task of ensuring technical harmonization for appropriate subject areas under the purview of the OSI Implementors Workshop, the European Workshop for Open Systems, and the Asia-Oceania Workshop. The fourth feature is that every attempt is made to reach agreements by unanimous consensus of all interested participants. The fifth feature is that the agreements are maintained in an appropriate manner to satisfy user requests.

The OSI Implementors Workshop is organized as a plenary and various Special Interest Groups (SIGs). Each SIG covers a different OSI functional study area. Each SIG is tasked by the plenary to do work under an approved charter, and submit this work to the plenary for ratification. Only work approved by the plenary is included in the Stable and Working Documents. The work must be of general benefit to vendors and users, and be related to the charter of the workshop (e.g., OSI data communications). Further information on the workshop may be obtained from the Computer Systems Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899 (ATTN: NIST Workshop for Implementors of OSI).

GOSIP as a primary source will reference relevant text in the Stable Document; when this is not appropriate, GOSIP may reference other sources as well (see sec. 3.3). Workshop documentation is public-domain and publicly available. It is not subject to copyright in the United States. Any user or individual may reference the Workshop Agreements. Not all text in the Workshop Agreements is necessarily referenced by GOSIP. Other user groups besides GOSIP reference the Workshop agreements. The schedule for progression of Workshop agreements is not linked to the schedule for progression of GOSIP or any other user group. Workshop attendees consider the content of the appendices of GOSIP for future planning of Workshop activities.

At the time a Federal Register notice for a new version of GOSIP is issued, a version of Workshop stable implementation agreements will be selected for that new version of GOSIP to reference. Relevant NIST personnel pay close attention to the recommendations of the Workshop in determining the effective dates of new functionality or errata to existing functionality. Interpretation ambiguities may be input back into the standards process for resolution.

Version 1 and Version 2 of GOSIP are based on Version 3 of the NIST/OSI Stable Implementation Agreements (NIST SP 500-177) [NIST 1]. The creation of a stable set of workshop agreements is a necessary step toward the assimilation of OSI products into the Federal environment.

Specifically, Version 2 of GOSIP references parts 2, 3, 4, 5, 7, 9, and 14 of Version 3 of the NIST Workshop Agreements For GOSIP procurements, Federal agencies should reference the appropriate part of the latest version of the NIST Workshop Agreements, because that version contains the latest errata and is publicly available. See section 4, Question 26 for additional information.

Workshop documentation is ordinarily distributed to Workshop attendees. In addition, the Stable Document (plus replacement pages) is available from several outside sources; consult the "references" section for ordering information. It is also planned to make this documentation available on-line. (Hereafter the Workshop will be referenced as the NIST/OSI Workshop.)

The RWS-CC (Regional Workshop Coordination Committee) meets several times a year to monitor progrss towards international harmonization of implementor agreements. Text technically harmonized as described above may be submitted to ISO/IEC through JTC1 as a proposed draft ISP (Internationally Standardized Profile). It is a goal that an ISP not compromise GOSIP interoperability.

3.2.3 MAP and TOP

Vendors are marketing products based upon OSI standards as refined by the NIST Workshop Agreements. User organizations must effectively represent the interests of the various user communities in (1) making their requirements known to vendors, and in (2) stimulating the vendors to produce products based upon those stated user needs A prominent example of such an organization is the MAP (Manufacturing Automation Protocol)/TOP (Technical and Office Protocol) Users Group. The MAP activities are focussing on

factory floor automation communications support and the TOP activities are focussing on non-manufacturing communication covering a broad range of activities such as administration, engineering, finance, and publishing. The MAP/TOP Users Group maintains close coordination between these two areas of activity in order to guarantee compatibility. MAP/TOP and GOSIP also strive to maintain compatibility between their specifications. In the future, a version of GOSIP and a MAP/TOP specification may be combined into one "document."

The reasons for this collaboration are obvious. A single set of user requirements covering both Government and industry needs means that small and large vendors have a larger market and that there is greater economic incentive for vendors to build interoperable OSI products.

Various public demonstrations of OSI implementations have been supported by the MAP/TOP Users Group, including the National Computer Conference in 1984 and Autofact in 1985. The purpose of these demonstrations was (and is) to show the feasibility and workability of OSI. An Enterprise Networking Event in June 1988 was the first major exhibition of OSI-based communications products in the United States. The recent "Interop 90" show included demonstrations of OSI products available from most computer vendors.

Although GOSIP has much in common with the goals of the MAP/TOP Users Group, there are differences which are reflected in the documents issued by the groups. The MAP [MISC 1] and TOP [MISC 2] specifications state what those organizations want the vendors to produce to meet their requirements, and MAP/TOP User organizations are encouraged to use the specifications as a basis for their OSI procurement requests. GOSIP is mandated for use in Government procurement requests; for that reason GOSIP references functionality which is available from vendors now or in the near future. However, the protocols in GOSIP have been carefully coordinated with the MAP and TOP organizations in order to insure that vendors can produce implementations based on a single set of user requirements. The MAP and TOP activities are currently administered by the Corporation for Open Systems International. For general information on MAP or TOP, write to:

Corporation for Open Systems International, 1750 Old Meadow Road, McLean, VA 22101-4306 ATTN: Strategy Forum Support.

3.3 GOSIP Summary

Version 2 of GOSIP has been issued as Federal Information Processing Standard (FIPS) 146-1 by the NIST. The history, nature, scope, and future of GOSIP are described below.

In late 1986, as the standards, NIST Workshop Agreements, and MAP/TOP user specifications were nearing stability, an effort was initiated to develop a U.S. Government OSI profile. Vendor OSI implementations were being completed and demonstrated, and commercially-available OSI products were being produced. The intent was (and is) for U.S. Government users to take advantage of these developments. Figure 5 illustrates this progression.

Goals of the GOSIP effort are: (1) to enable Federal users to select optimal OSI protocols and options from among a wide variety of choices, (2) to define a single Federal user community to vendors, and (3) to transmit Federal user requirements to vendors, as well as to encourage vendors to build OSI products satisfying these requirements. The commitment of GOSIP is to achieve multi-vendor interoperability in the Federal workplace.

Through collaboration among a small group of U.S. Government technical experts, a draft specification was produced in December 1986. The GOSIP initial specification has undergone successive cycles of review and comment. All Federal agencies and interested organizations were invited to comment; these same organizations provided valuable input back into the revision process. All segments of the U.S. Government were consulted during the preparation of GOSIP Version 1 and GOSIP Version 2.

NIST recommends the final content of GOSIP to the Secretary of Commerce for approval, and maintains

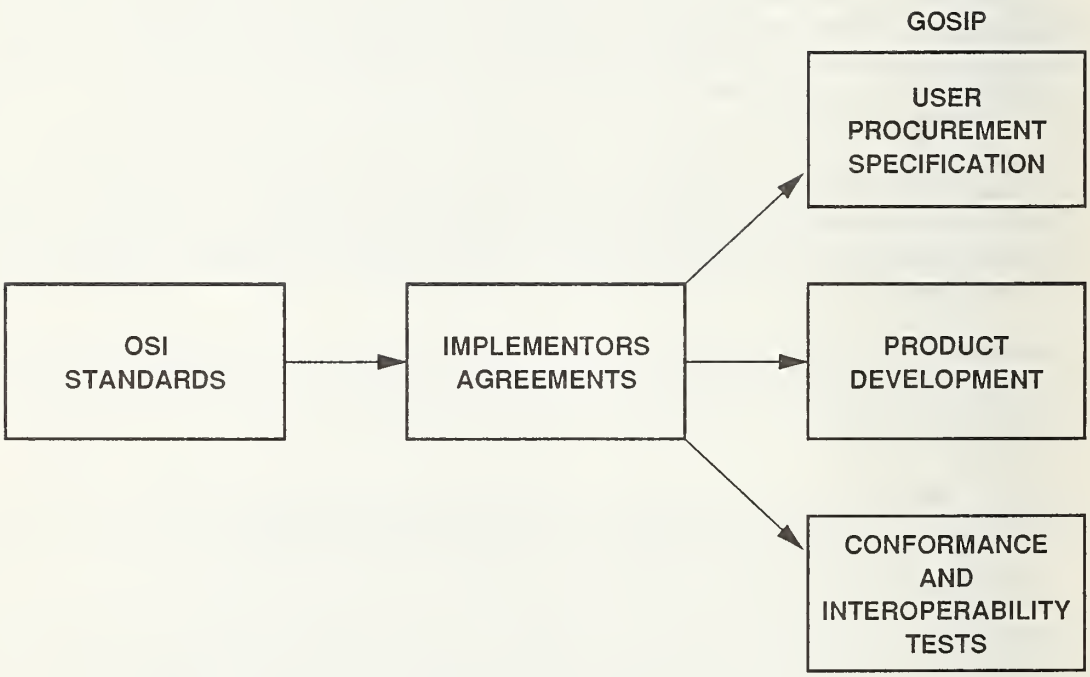


FIGURE 5
GOSIP CONTEXT

and updates the GOSIP documents. A review period is provided to allow public comment on proposed changes to GOSIP. New versions of GOSIP are developed and proposed at intervals that reflect the availability of significant additional services provided by OSI applications that meet Federal needs.

The FIPS for GOSIP consists of three parts: (1) a technical specification (version 2), which contains information on the OSI protocols and services provided, (2) information on applicability and implementation of the FIPS, and (3) appendices describing future GOSIP requirements and plans for meeting such requirements. After extensive government and industry review, GOSIP Version 1 was promulgated as a FIPS (FIPS 146) in August 1988. GOSIP applies to all U.S. Government agencies around the world. Other organizations of a similar nature (e.g., State governments) may decide to adopt GOSIP for their programs as well. The NIST edits the contents of the GOSIP FIPS, with advice and consultation coming from other Federal agencies. Drawing on the technical contributions of these agencies, the NIST prepares GOSIP, has it reviewed, responds to comments from government and industry, and recommends that the Secretary of Commerce approve it as a FIPS.

Version 1 of GOSIP is mandatory from August 1990. GOSIP represents a significant resource which may be referenced by both inexperienced and sophisticated OSI users. Products containing OSI functionality referenced in Version 2 of GOSIP are currently available. Version 2 of GOSIP contains all of the protocols that appear in Version 1 of GOSIP plus the additional protocols that have been implemented by vendors since Version 1 was created. Federal agency personnel should reference the latest version of GOSIP in all procurement requests. It is important to emphasize that the GOSIP process reflects a long-term strategic initiative, as manifested in the latest GOSIP FIPS.

The GOSIP FIPS is updated by issuing new versions at appropriate intervals to reflect the progress being made by vendors in providing OSI products with new services useful to Federal agencies. A new version of GOSIP supersedes the previous version of the document because it includes all of the protocols in the previous version plus additional new protocols. Procurement of the new protocols is mandated in Federal procurement requests initiated 18 months after the version of GOSIP containing those protocols is promulgated as a FIPS. Each new version of GOSIP specifies the architecture and protocols that were included in each of the previous versions so that Federal agencies can easily determine the applicable compliance date for each of the protocols.

It is a goal that a new version of GOSIP be compatible with the previous versions. However, changes may be required to correct errors and to align with activity in the international standards organizations. Any errata required to a previous version of GOSIP are identified in the new GOSIP version. Section 1.7 of GOSIP Version 2 identifies GOSIP Version 1 errata. Unless otherwise stated, the mandatory compliance date of the previous version of GOSIP also applies to the errata. These errata are not included without ensuring that they have the strong support of the vendors who are providing OSI products so that users can be confident that these changes will not inhibit interoperability. In each new version of GOSIP, only the added networking services carry a new mandatory compliance date. The promulgation of new versions of GOSIP is announced in a Federal Register notice. The appendices of GOSIP describe functions which may be included in future versions of GOSIP. Sources of material for GOSIP are as given in section 1.8 of the GOSIP FIPS.

Testing of GOSIP protocols is an important component of the GOSIP process. Additional information on GOSIP testing, as well as a statement of the GOSIP test policy, is given in section 6.

3.4 Future of GOSIP

Each new version of GOSIP is developed in conjunction with the GOSIP Advanced Requirements Group, a group of technical experts appointed by Federal agencies. As OSI activity progresses in the international standards organizations and the NIST/OSI Workshop, the GOSIP Advanced Requirements Group recognizes this work and develops a schedule for including it in a future version of GOSIP. A tentative schedule for including additional OSI functionality is given in the Appendices of each GOSIP version. It is a goal to include new GOSIP functionality as quickly as possible, and to ensure that these inclusions are consistent

with current GOSIP technology.

This new functionality includes network security, network management, IS-IS dynamic routing, directory services, electronic data interchange, transaction processing, and remote database access. In addition, steps are underway to enhance the capabilities of applications currently in GOSIP. See section 7 for a detailed description of important new work items.

In the future OSI functionality referenced by GOSIP will grow to reflect additional Federal user requirements. Future versions of GOSIP, issued no more frequently than once per year, will define new OSI functionality, while "building" on the material in previous versions. The work of the international standards organizations and the NIST/OSI Workshop will be fed into the GOSIP creation process. Experience gained by Federal users in GOSIP product assimilation will be input into future GOSIP versions to constantly improve the quality of the document. Requirements of the MAP and TOP groups will also continue to be considered in developing GOSIP.

Procedures and mechanisms are being put in place to ensure proper management of GOSIP evolution and related testing issues. The concerns of users, vendors and suppliers will all be input into these mechanisms.

3.5 International Cooperation

Worldwide alignment of government functional profiles (such as GOSIP), where appropriate, is important to create a large consolidated market for vendor OSI products; thus, the availability of OSI technology is improved. Such alignment would support the feasibility of international recognition of tests, testing methods, and test results. In support of alignment, efforts are underway to: (1) identify differences between the profiles of various governments around the world, with a view towards resolving the differences, (2) establish harmonization of functional profiles under the supervision of the RWS-CC (see sec. 3.3), and (3) develop tools for application to automated implementation and testing of protocols using a formal specification as a base. These efforts should be supported.

An organization called the IPSIT (International Public Sector Group for Information Technology) is exploring areas of cooperation among various government procurement specifications around the world. Countries which are developing or have developed OSI profiles are: Canada, Australia, Norway, the United Kingdom, France, Germany, Sweden, Japan, Korea, and Israel. Other user concerns (such as those involved with library applications and medical data transfer) are being identified in relation to GOSIP. Thus, GOSIP is part of a worldwide collaborative effort involving OSI.

4.0 GOSIP QUESTIONS AND ANSWERS

Listed below are answers to some of the most commonly asked questions concerning GOSIP.

QUESTION 1: Does Version 2 of GOSIP (FIPS 146-1) supersede Version 1 of GOSIP (FIPS 146)? What is the best method of accessing the information that I need to comply with the GOSIP Version 1 mandate?

ANSWER: Version 2 of GOSIP supersedes Version 1 of GOSIP, and should be used as the sole GOSIP reference. Version 2 of GOSIP includes all GOSIP Version 1 protocols plus additional protocols that are new to Version 2

Version 2 of GOSIP clearly distinguishes the GOSIP Version 1 protocols which are mandated now in Federal procurements from the GOSIP Version 2 protocols which will be mandated in Federal procurements initiated after October, 1992.

Another reason for users to reference Version 2 of GOSIP is that Version 2 of GOSIP contains GOSIP Version 1 errata These errata apply to the GOSIP Version 1 mandate, but are not included in the Version 1 document.

QUESTION 2 Does GOSIP apply to all procurements of computer network products? If not, to what procurements does it apply?

ANSWER GOSIP does not apply to the procurement of all computer network products. GOSIP must be cited in solicitations and contracts when the systems and services to be acquired provide functions equivalent to those specified in the GOSIP document.

Version 1 of GOSIP allows users to send and receive electronic mail using the Message Handling Systems (MHS) protocol, and allows users to access and transfer information files using the File Transfer, Access, and Management (FTAM) protocol. In addition, Version 1 provides a reliable end-to-end service between computer systems served by different network technologies. Version 1 of GOSIP was effective in February 1989, and was mandatory in August 1990. Version 2 includes additional protocols not included in Version 1, such as the virtual terminal service which allows a terminal and remote host to have an interactive conversation. Procurement of the new protocols is mandated in 1992, 18 months after Version 2 of GOSIP was promulgated as a FIPS Each new version of GOSIP specifies the architecture and protocols that were included in each of the previous versions so that Federal agencies can easily determine the applicable compliance date for each of the protocols. Federal agencies are encouraged to reference Version 2 GOSIP functionality in procurement requests which originate before the Version 2 of GOSIP is mandatory. For more discussion on GOSIP applicability, see section 5.

QUESTION 3: How can an agency effectively make the transition from its existing systems to the use of GOSIP-compliant products?

ANSWER: There is no single strategy for integrating GOSIP compliant products with existing systems which will apply to all agencies. The most effective solution will vary with current protocol architecture(s) and the configuration of existing system(s). Some alternatives to consider include the use of dual protocol hosts, application and network layer gateways, and mixed protocol stacks. These alternatives are more fully described in section 9. Current vendors should be consulted in planning a transition strategy. The Department of Defense (DOD) has developed and documented an excellent OSI implementation plan [DOD 4].

QUESTION 4: Will there be future versions of GOSIP? How often will they be issued? Can it be told in advance what is likely to be included in the new versions?

ANSWER: A draft of Version 3 of GOSIP is planned for early 1992. Subsequent versions will be issued no more frequently than once a year; a more likely interval is every 18-24 months. It is a goal to make each new version backwardly compatible with the previous version. Notice of any exceptions to this rule will be published for public comment in the Federal Register. The latest version of GOSIP publicly available should be referenced. The appendices of GOSIP give a complete summary of the protocols planned for inclusion in future versions of the document.

QUESTION 5: Who decides what functionality to include in each new version of GOSIP?

ANSWER: The NIST is responsible for the content of each new version of the GOSIP FIPS. The GOSIP Advanced Requirements Group, consisting of Federal agency technical experts, provides assistance and technical input into the specification. The comments of manufacturers, Government agencies, and the public are then solicited. The GOSIP Advanced Requirements Group will consider the technical comments and may recommend revisions to a GOSIP version. Drawing on technical contributions from the GOSIP Advanced Requirements Group, the NIST prepares the specification, ensures its review, and recommends that the Secretary of Commerce approve the resulting version as a FIPS.

QUESTION 6: How does the GOSIP Advanced Requirements Group recommend functionality to include in each new version?

ANSWER: The GOSIP Advanced Requirements Group discusses and makes recommendations to the NIST as to which OSI protocols provide services that meet Government needs. The progress made in developing an international standard and implementors agreements for each of these protocols is monitored. Since GOSIP will be referenced by procurement authorities, the GOSIP Advanced Requirements Group also verifies that implementations of these protocols will be available from vendors at the time or soon after the protocol is included in GOSIP. When the GOSIP Advanced Requirements Group completes its recommendations on additions to GOSIP, the NIST incorporates the technical comments into proposed standards which are reviewed by government and industry.

QUESTION 7: How can I know that the OSI product that I am procuring complies with GOSIP?

ANSWER: The NIST has selected the abstract test suites and test systems to be used in verifying GOSIP compliance, as well as the test laboratories which can perform appropriate tests. OSI vendors can have their products tested at accredited laboratories and, if the results are successful, the products will be registered as GOSIP compliant. The NIST will publish, on a quarterly basis, lists of registered GOSIP products. Additional information on testing is given in section 6.

QUESTION 8: Which is more important, conformance testing or interoperability testing?

ANSWER: Both are important. Conformance testing provides the most thorough evaluation of an OSI implementation and is mandated for a vendor who wants to claim GOSIP compliance. Testing organizations, however, do not claim that conformance testing can detect all errors or provide guarantees of interoperability. The NIST mandates that interoperability testing with a GOSIP reference implementation be performed when

reference implementations exist. However, since no such implementations are likely in the near future, the NIST recommends that interoperabiltiy testing be performed between products built by different suppliers, and that agencies require assurance of interoperability. The NIST is accrediting the testing services that will verify the interoperability of GOSIP conformant products.

QUESTION 9: What kind of testing is reasonable and practical for an agency to conduct on its own?

ANSWER: Full seven layer interoperability testing of OSI applications can easily be performed by most users. The NIST has published interoperability tests for MHS [NIST 9] and FTAM [NIST 10], which were originally developed by a group of OSI suppliers and users called OSINET. The tests were coordinated with organizations in other parts of the world in order to get international concurrence. The tests exercise a full range of functionality for those applications and can be run by users that have a minimum of OSI knowledge.

QUESTION 10: If many GOSIP-compliant products exist, how can I tell which product meets the needs of my agency?

ANSWER: The NIST is publishing a series of documents to assist users in evaluating different implementations of the OSI applications. Guidelines for evaluating MHS implementations [NIST 3] were produced in 1990; guidelines for evaluating FTAM implementations will be available in 1991. The guidelines for each OSI application will describe how an implementation can differ in the functional and performance capabilities offered to the user. Users will be able to match their requirements with the services provided by existing implementations. An algorithm to assist in the rating process will be provided.

QUESTION 11: What should be an agency policy concerning the procurement of OSI products for which accredited conformance and interoperability tests are not yet available?

ANSWER: Agencies should not hesitate to purchase OSI products if certified conformance and interoperability tests are not yet available. Most of these products have undergone thorough testing on an informal basis; interoperability testing has been demonstrated through vendor participation in OSINET and in major trade shows. Agencies can require that the successful vendor provide proof of GOSIP compliance some number of months after the testing services which measure conformance and interoperability are available.

QUESTION 12: An agency is procuring a system which provides directory services. Since directory services is not included in Version 2 of GOSIP, is it true that GOSIP should have no impact on that agency's procurement actions?

ANSWER: The GOSIP appendices should be consulted to determine whether the application functionality that is being procured will be included in a future version of GOSIP. If this functionality is scheduled for inclusion, it would be a mistake not to be forward-looking in a procurement action.

Systems conforming to international standards that provide directory services may be widely available at the time that the system that is being procured is delivered, certainly during the expected lifetime of that system. Contract solicitations should insist that vendor proposals include a plan for making the transition to GOSIP-compliant products.

QUESTION 13: What are the guidelines for requesting a waiver from GOSIP compliance? What are

the procedures for requesting such a waiver?

ANSWER: A waiver from the GOSIP Federal Information Processing Standard may be requested when compliance would adversely affect the accomplishment of the mission of a Federal agency or cause a major adverse financial impact which is not offset by Government-wide savings. For additional waiver guidelines and procedures, consult section 5.4.

QUESTION 14: How can one acquire the knowledge of OSI protocols that is needed in order to make intelligent procurement decisions?

ANSWER: The GOSIP Users' Guide is intended as a first step in providing Federal personnel with the information that they need to make these decisions. In addition, the NIST will hold seminars on GOSIP-related issues from time to time. Commercial organizations will also conduct classes on the OSI architecture and on specific OSI protocols. However, most Federal agency personnel will find that they do not need to be an expert on the technical details of each OSI protocol. In most cases, an understanding of the services offered by the protocols and how the services relate to the mission of their agency is sufficient.

QUESTION 15: What is the relationship of GOSIP to the MAP and TOP specifications?

ANSWER: GOSIP is consistent with and complementary to industry's Manufacturing Automation Protocol (MAP) and Technical and Office Protocol (TOP). Both MAP/TOP and GOSIP share the common goal of conveying user requirements to the vendor community, in order to facilitate the development and procurement of interoperable OSI products. However, the GOSIP document is mandated for use by the Federal procurement authorities, whereas the MAP and TOP specifications are considered a strong recommendation but not a mandate for those organizations.

QUESTION 16: If OSI protocols are installed on an agency's computer systems, will communication be possible with all other computers?

ANSWER: No. Open System Interconnection (OSI) protocols define a standard language for communicating data between computer systems, but all computer systems wishing to communicate must speak the same standard language. OSI is analagous to defining a standard natural lauguage (e.g., ESPERANTO) for human-to-human communication. Each speaker then need only know his/her native language and the standard language in order to communicate within the speaker's local community and throughout the world. Thus, if every computer system in the world used OSI protocols, computer systems could, in principle, communicate with all other computers, provided security requirements were met and no OSI dialects existed to hinder interoperability.

The true advantages of adopting GOSIP within a computing environment derive from interoperability among computers made by different vendors. The computing environment in Government is increasingly heterogeneous for three reasons: (1) specialists provide superior price-performance in niche markets such as engineering workstations, supercomputers, and disk servers, (2) cheaper computing power allows users to make autonomous buying decisions at lower levels in an organization, only to face later requirements to interconnect, and (3) competitive procurements lead to natural variety among computer suppliers.

In the absence of a data communications standard, the environment created is analogous to a workplace where each worker speaks one, or at most two, of six or seven natural languages. Communication becomes difficult and expensive. Settling upon GOSIP as a standard for data communications within a working environment will enable cost-effective interoperability among a variety of computers.

QUESTION 17: Is GOSIP intended to limit the network technologies available to Government users?

ANSWER: No. GOSIP defines a limited set of standard network interfaces, commonly available as products, for connecting computers to networks. These network interfaces include: (1) packet-switched network (X.25), (2) carrier sense multiple access with collision detection (IS 8802/3), (3) token bus (IS 8802/4), (4) token ring (IS 8802/5), and (5) Integrated Services Digital Network (ISDN). While these standard network interfaces are commonly supported by specific network technologies, other arrangements are possible. For example, the IS 8802/3 interface may provide connection to a programmable branch exchange (PBX) using cut-through routing to provide a connectionless data service. The computer system connecting to the 8802/3 interface is unaware that a PBX is the network technology moving the data. The use of the PBX in providing an IS 8802/3 interface is compliant with GOSIP.

GOSIP also permits considerable flexibility with respect to the physical interface. For example, connections to X.25 networks may support RS232, RS530 or V.35 depending on speed and distance requirements. As a second example, IS 8802/3 interfaces may be provided using fiber optics techniques, or, technology permitting, twisted-pair telephone wiring.

GOSIP is intended to enable Government users to take advantage of several commonly available vendor products for connecting to networks; however, the true interoperability provided by GOSIP is end-to-end at the Transport Layer with network interconnection provided by the Connectionless Network Protocol (CLNP). The CLNP is used to interconnect a wide variety of standard and nonstandard networks and the Transport protocol is used to provide a reliable end-to-end data path between computers across interconnected networks. Such a reliable end-to-end data path may be used by a wide range of GOSIP application services (e.g., MHS, FTAM and VT) and non-GOSIP applications (e.g., Network File System).

QUESTION 18: Can ISDN be used with GOSIP?

ANSWER: Yes. In GOSIP Version 2, text is included to connect computer devices directly to ISDN switches without requiring an X.25 terminal adapter. In GOSIP Version 2, ISDN can provide an alternative subnetwork technology for GOSIP end systems, as well as function as an intermediate subnetwork between other subnetwork types.

QUESTION 19: Is GOSIP intended to mandate OSI protocols for every Government PC (personal computer)?

ANSWER: No. PCs are small host computers, and GOSIP protocols may be used to provide networking services for PCs; however, several other methods of using PCs in conjunction with GOSIP are possible. For example, GOSIP mail and file transfer services may be made available on minicomputers and/or mainframes accessible to PC users via remote login procedures over serial lines. The placement of GOSIP services within a local systems environment is a technical issue to be decided based on cost and functional requirements, and is beyond the scope of the GOSIP FIPS.

QUESTION 20: If GOSIP protocols are implemented, will computer systems be more vulnerable to unauthorized access?

ANSWER: No. While the interconnection of computers via communication links provides increased opportunity for external intrusion, the use of the GOSIP protocols does not increase the level of vulnerability.

Existing standard protocols, such as the TCP/IP suite, are no more or less secure than the newly adopted GOSIP protocols. Work is underway within Government and industry to develop and implement security protocols for use with GOSIP; in fact, a future version of GOSIP will include such security provisions. In the interim, section 6 of the GOSIP FIPS defines a security option for use with the CLNP.

QUESTION 21: Are OSI protocols equivalent to X.25?

ANSWER: No. OSI protocols provide a broad range of network services, historically divided into seven functional layers - the OSI Reference Model. X.25 is a standard defining a protocol for use within the OSI network and link layers. Many other protocols are available to fill out the services in all seven layers of the OSI Reference Model; thus, X.25 is one of the OSI protocols, and is designed to provide specific functionality within several adjacent layers of the OSI Reference Model.

QUESTION 22: Does GOSIP provide programmer-accessible interfaces to network services?

ANSWER: No. GOSIP enables users to purchase products that provide INTEROPERABLE networking services in a multi-vendor environment. For example, GOSIP protocols enable users to send electronic mail to remote users without concern for the type of computer or mail program the receiving user owns. The GOSIP also permits users to transfer files between machines without user concern for incompatibilities in hardware architecture or file system structure. GOSIP enables INTEROPERABILITY between computers.

GOSIP neither mandates nor defines any programmer-accessible interfaces to the network services. Such interfaces may prove useful to achieve SOFTWARE PORTABILITY for programs requiring network services. If a user requires an interface to specific GOSIP-compliant network services, the user must say so in a request for proposal (RFP). If a user desires software portability for programs that use the programmatic interfaces sought in an RFP, the user must not only specify that an interface is required, but also must specify the precise characteristics of the interface. If the interface is not precisely defined, each vendor may provide a different functional interface of the required type. GOSIP IMPLEMENTATION ALONE DOES NOT ENABLE APPLICATION PORTABILITY.

Late in 1988 the IEEE formed a subgroup within the POSIX (Portable Operating System Interface for Computer Environments) standards group to address the issue of POSIX networking. This subgroup is divided into six working groups to develop different standard interfaces; other working groups may be added. For more information see section 10.2.5.

QUESTION 23: Does GOSIP specify user interfaces to network applications?

ANSWER: No. As described above, GOSIP enables INTEROPERABLE NETWORKING SERVICES between computers made by different manufacturers. In many instances, computer manufacturers add GOSIP services to pre-existing proprietary services without perceptable change to the end user. For example, a user editing and sending mail from a terminal with a proprietary mail package might follow exactly the same set of keyboard actions and witness the same display responses when the GOSIP X.400 (MHS) mail protocol is invoked to relay and deliver the completed message. The user interface is an area where vendors will continue to differentiate their products from those of competitors.

GOSIP neither mandates nor defines any user interfaces to network applications. Such interfaces may prove useful to achieve user portability between computers when network applications are required. If a procuring agency requires a specific user interface to network applications, the details of the interface must be specified. The specification must be included with the RFP. GOSIP ALONE DOES NOT DEFINE ANY

PARTICULAR INTERFACE TO NETWORK APPLICATIONS.

QUESTION 24: Are GOSIP-compliant products available?

ANSWER: Yes. Almost every major U.S. computer vendor has announced availability of some GOSIP-compliant products. Transport Layer products were available as early as 1984. CLNP products made a market appearance in 1985. Session Layer products are also available. A variety of local and wide area network products complying with GOSIP, as well as full seven layer implementations of Message Handling Systems and File Transfer, Access and Mangement, are widely available. A full range of GOSIP-compliant products, integrated across vendor product lines and including gateways with proprietary offerings, should be available from most major computer vendors when the GOSIP FIPS makes their procurement mandatory. Contact computer vendors for specific product offerings and future plans.

QUESTION 25: Will GOSIP-compliant products cost more than other solutions for data communications?

ANSWER: No. Although vendor pricing strategies are made after considering a large number of business factors, nothing inherent in GOSIP protocols requires compliant products to be more expensive than vendor proprietary offerings; in fact, several factors suggest that long-run pressures will push prices down.

One such factor is implementation variety. GOSIP mandates protocols for interoperable data exchange. Vendors may offer a range of solutions, complying with GOSIP, designed to vary in price. With basic interoperability assured, users may trade price for performance more easily.

A second price suppression factor is alternative sourcing. With GOSIP-compliant products available from a variety of vendors, users may cost-effectively switch to lower-cost vendors without losing interoperability.

A third factor is basic interoperability itself. When a vendor is required to connect equipment with an installed base from a different vendor, use of a GOSIP-compliant solution is likely to be cheaper than implementation of a custom solution.

QUESTION 26: What version of the NIST Workshop Agreements should Federal agencies reference?

ANSWER: Version 2 of GOSIP originally referenced Version 3 of the NIST Workshop Agreements, because that was the latest version existing at that time. For GOSIP procurements, however, Federal agencies should reference the appropriate part of the latest version of the NIST Workshop Agreements because that version contains the latest errata, and only that version is publicly available. For example, in 1989 eight technical errata were added to FTAM Phase 2 functionality (see sec. 7), and in 1990, one technical erratum was added. It is necessary to reference the latest version of the NIST Workshop Agreements in order to reference these and other errata that have been added since Version 3 of the NIST Workshop Agreements was published.

If major new functionality (e.g., Phase 3 vs. Phase 2 FTAM, 1988 MHS vs. 1984 MHS) is added to an existing protocol, the agreements for this functionality will appear in an entirely new part of the NIST Workshop Agreements, and might be included in some future version of GOSIP. See section 3.2.2 for more information on the NIST/OSI Workshop.

5.0 GOSIP APPLICABILITY ISSUES

5.1 Introduction

An important decision for Federal agencies is the extent to which GOSIP applies to their particular situations. Given that GOSIP provides economic and planning benefits to users (as explained in sec. 2), it makes sense for every U.S. Government organization to adopt a policy to implement it in future procurements. Answers will be given in this section to the questions of when and how to apply GOSIP. The OSI protocols specified in GOSIP free users from dependence on a single vendor for new network products and services and promote interoperability across a multi-vendor environment.

Section 2 outlined compelling reasons for an agency to adopt the OSI concept as a strategic initiative; however, each agency is aware of its particular ADP environment and configurations, and each has a unique administrative and political perspective. After reading this section, a user should be able to determine the full extent of GOSIP applicability in a particular environment.

GOSIP should be employed in an agency procurement, planning, and implementation program which involves all ADP and data communications configurations within an agency. The above is true for two reasons: (1) GOSIP provides communications functionality that will meet the requirements of nearly every computer configuration, and (2) GOSIP provides enhanced interoperability.

The approach taken in this section is a deliberate one. First, a broad statement of applicability will be given, emphasizing development of the strategic initiative from section 2. Following this, configuration information will be given. Next, a discussion of waivers and policy decisions will be presented. GOSIP enforcement will be discussed third. After this, specific applicability recommendations are given for Federal agencies. Finally, specific questions will be raised, and answers given, to pertinent concerns and questions users may have regarding GOSIP applicability.

5.2 General GOSIP Applicability

GOSIP Version 2 was issued on April 3, 1991. The mandatory compliance date of Version 2 of GOSIP is October 3, 1992. Federal agencies are encouraged to reference GOSIP in procurement documents before the mandatory compliance date is reached.

GOSIP Version 1 was mandatory in August 1990. GOSIP should be applied as part of a broad comprehensive strategic acquisition plan embraced by an agency at the policy level. In light of the benefits of OSI described in section 2, it is anticipated that GOSIP will be applied in most instances where there is a choice.

GOSIP applies to new networking systems which will be procured, and to major upgrades to existing networks. Units operating with existing, non-GOSIP networks should add GOSIP-related components into networking systems when such components are available, cost-effective, and efficient for the organization's operation. It is anticipated that with GOSIP all of these conditions will be met.

Since GOSIP deals with communications functionality, and not specific ADP configurations (see sec. 5.3), GOSIP functionality is not bound to any hardware, software, or operating system limitations. This means that GOSIP may apply to all types of systems, in all types of environments. The size of the system is not important in the context of GOSIP; neither is the communications medium used. GOSIP functionality may be implemented in different ways (see sec. 7).

There are three general criteria for GOSIP applicability, as follows: (1) the communication must be "computer-to-computer" (that is, between two or more intelligent systems that are able to exchange information), (2) the communicating systems must be autonomous, and (3) the communications functionality must be contained in GOSIP. GOSIP applies to communications between systems, and the use of GOSIP for communications between system components is encouraged where applicable, particularly for distributed

systems. Figure 6 gives examples of situations in which GOSIP may be applied.

GOSIP provides two basic capabilities. First, it enables users to request standard applications operating over standard networks. The standard applications supported in Version 2 of GOSIP are File Transfer. Access, and Management (FTAM) [ISO 2-6], Message Handling Systems (MHS) [CCITT 2-9], and Virtual Terminal [ISO 7-8]. Standard network technologies supported include IS 8802/3 (CSMA/CD) [ISO 9], IS 8802/4 (token bus) [ISO 10], IS 8802/5 (token ring) [ISO 11], X.25 wide area network [CCITT 1], and ISDN [CCITT 11-13]. For further explanations, see section 7. For example, an MHS user on an 8802/3 network may send a message to an MHS user on an 8802/4 network; these networks may be interconnected by an X.25 network. Second, GOSIP provides a reliable end-to-end service over which users can write their own applications. For example, a nonstandard application to exchange office documents may use the GOSIP end-to-end reliable transfer service, which is provided by OSI layers 1 through 4 (see sec. 7). Obviously, this application must satisfy the conventions of the Transport Service Definition.

The important point is that GOSIP has been deliberately designed to provide a generic set of functionality which may be used in almost any system. Furthermore, it gives a great deal of flexibility to users. Standard networks may be joined to create a large GOSIP-compliant internetwork. In sum, subject to the above constraints, GOSIP generally applies to any ADP environment.

5.3 Configuring a GOSIP System

GOSIP systems can be configured using a "building block" approach. This strategy allows GOSIP systems to be adapted to a specific user requirement.

For example, GOSIP, in layers 1-4, provides a service which allows end systems on one subnetwork to reliably transfer data to end systems on other subnetworks. This reliable transfer service is a foundation upon which a user can develop protocols which do not conform to an international standard but do meet a specific user need. The reliable transfer service, in turn, can use a Connectionless Network Service which masks the differences between various network technologies and allows the transfer of data among different subnetworks, or, optionally, use a Connection-Oriented Network Service to transfer data more efficiently when all end systems are attached to X.25 or ISDN subnetworks.

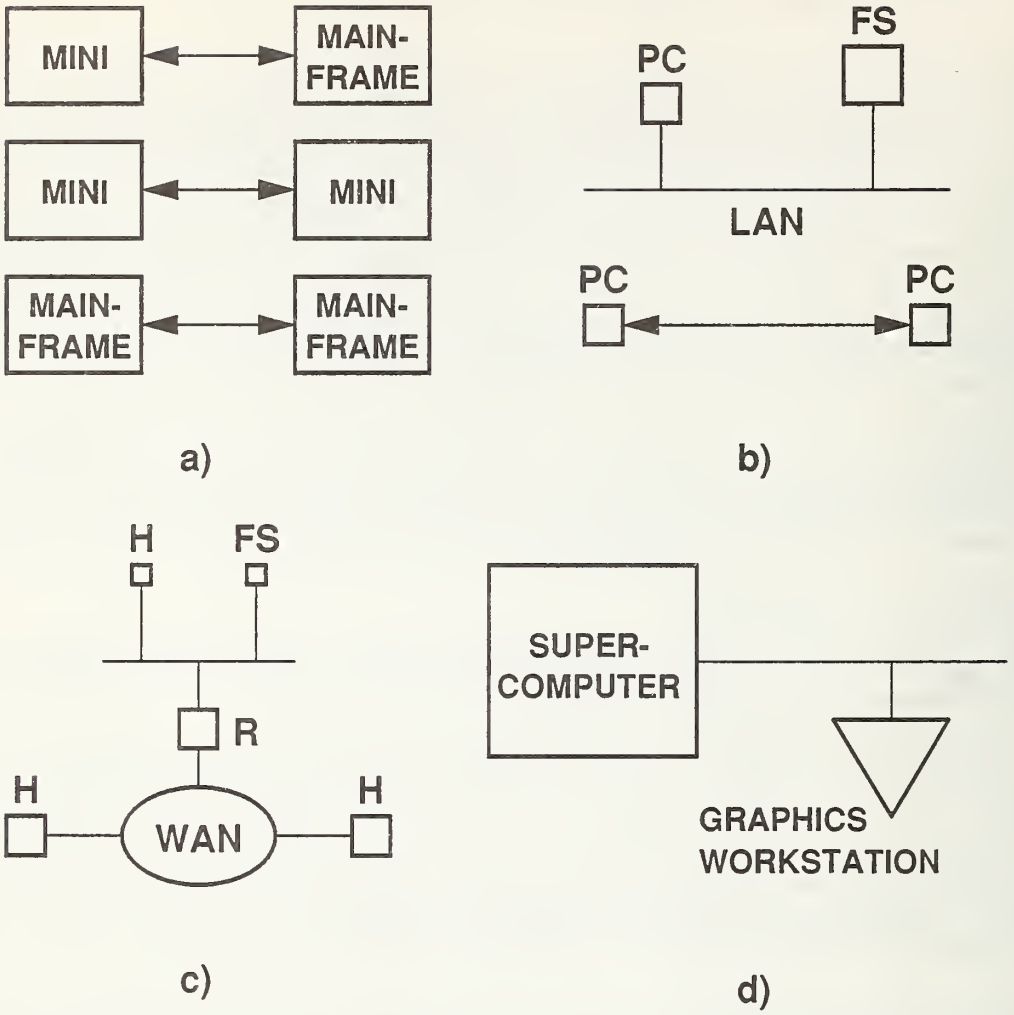
Other building blocks are available. At the Application Layer, the Association Control Service Element (ACSE) is designed to provide common Application Layer services which currently include the management of connections. The ACSE performs all required interactions with the Presentation Layer.

The CCITT, when developing the 1984 Recommendations for Message Handling Systems, recognized that the Message Transfer Service (MTS) could be used to transfer other than interpersonal messages. While standardizing an Interpersonal Messaging User Agent, they also standardized the interface between any user agent and the MTS. Thus, the same interface can be used by other User Agents which perform completely different functions (e.g., the transfer of process control information in binary form). The CCITT is standardizing an Electronic Data Interchange User Agent which accesses the MTS to send and receive business information.

These building blocks are not provided automatically in a GOSIP implementation. GOSIP does not constrain the way that vendors implement functionality; in fact, the merger of two or more OSI layers may provide a more efficient implementation. Users that want to make use of the capabilities provided by these building blocks must specify program interfaces to the appropriate layer(s) in their procurement requests.

5.4 Waivers and Policy Decisions

A waiver is an exemption from the requirement to purchase GOSIP-compliant products. Once a decision has been made to request a waiver, a procedure must be followed. This subsection will give all information necessary to request a waiver from using GOSIP.



H = HOST
R = ROUTER
FS = FILE SERVER
PC = PERSONAL COMPUTER
WAN = WIDE AREA NETWORK
LAN = LOCAL AREA NETWORK

FIGURE 6
EXAMPLES OF
GOSIP APPLICABILITY

Heads of agencies may waive the requirements of GOSIP in instances where it can be clearly demonstrated that there are significant performance or cost advantages to be gained and when the overall interests of the Federal Government are best served by granting the waiver. Waivers may be requested when functionality critical to an agency mission is not included in GOSIP-compliant products. Waivers may also be requested for special-purpose networks which are not intended to interoperate with other networks, or for products supporting network research.

A waiver request should describe in detail the reasons for the waiver. It should also include a description of the systems being purchased, and a length of time during which the waiver will be in effect. It should be noted that functionality which is not in the current version of GOSIP may be in a future version; thus it is recommended to reconsider the validity of an existing waiver in the future. Adjudication of waiver requests lies entirely within a particular agency. A decision will be made on the merits of the waiver. If a waiver is granted, agencies will be able to purchase alternative (non-OSI) systems, instead of GOSIP systems, for the duration of the waiver. If it is denied, agencies must find a way to translate their requirements into OSI-compliant systems.

A waiver may be requested at any point in the life cycle of a system, and at any relevant point in the procurement cycle. Application may be made by technical or procurement individuals within an agency. It is recommended that a template or standard series of forms be provided by each agency for waiver requests.

For the waiver management process, it is recommended that each agency: (1) appoint a custodian of waiver requests and actions, and (2) develop a procedure for exercising control over the waiver management process. It is further recommended that waiver requests be made in writing, and that actions taken (with reasoning included) be deposited in a single location within each agency. It is advisable that procedures for appeals of waiver decisions be developed within each agency.

It is recommended that a request for a waiver generated within an agency should include:

(a) a description of the existing or planned ADP system for which the waiver is being requested,

(b) a description of the system configuration, identifying those items for which the waiver is being requested, and including a description of planned expansion of the system configuration over its life cycle, and

(c) a justification for the waiver, including a description of the disadvantages that would result through conformance to this standard as compared to the alternative for which the waiver is requested.

The procedures for waivers are given below. Under certain exceptional circumstances, the heads of Federal departments and agencies may approve waivers to Federal Information Processing Standards (FIPS). The agency head may redelegate such authority only to a senior official designated pursuant to section 3506(b) of Title 44, U.S. Code. Waivers shall be granted only when: (1) compliance with a standard would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or (2) cause a major adverse financial impact on the operator which is not offset by Government-wide savings.

Agency heads may act upon a written waiver request containing the information detailed above. Agency heads may also act without a written waiver request when they determine that conditions for meeting the standard cannot be met. Agency heads may approve waivers only by a written decision which explains the basis on which the agency head made the required finding(s). A copy of each such decision, with procurement sensitive or classified portions clearly identified, shall be sent to: National Institute of Standards and Technology; ATTN: FIPS Waiver Decisions, Technology Building, Room B-154; Gaithersburg, MD 20899.

In addition, notice of each waiver granted and each delegation of authority to approve waivers shall be sent promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register.

When the determination on a waiver applies to the procurement of equipment and/or services, a notice of the waiver determination must be published in the Commerce Business Daily as a part of the notice of solicitation for offers of an acquisition or, if the waiver determination is made after that notice is published, by amendment to such notice. A copy of the waiver, any supporting documents, the document approving the waiver, and any supporting and accompanying documents, with such deletions as the agency is authorized and decides to make under 5 U.S.C. Sec. 552(b), shall be part of the procurement documentation and retained by the agency.

It is recommended that all approved waivers be considered interim measures and assigned an expiration date by agency heads (or equivalent officials). It is also recommended that waivered systems be brought into compliance with the present or future GOSIP specification, if possible, and that all waiver requests include information explaining when and how the subject systems will move to the OSI standards. As stated above, all waiver-related documents will be part of the agency procurement documentation and must be retained by the agency.

5.5 GOSIP Enforcement Issues

The Brooks Act (Public Law 89-306) establishes a government-wide program for the development of Federal Information Processing Standards (FIPS) by the NIST. Standards developed by the NIST are approved by the Secretary of Commerce and used by Federal Government agencies. GOSIP Version 2 has been approved by the Secretary of Commerce as FIPS 146-1, and enforcement will begin with agency solicitations issued when this GOSIP FIPS is mandatory. Enforcement will continue from that point onward, in the manner prescribed by the language of the FIPS, modified by any subsequent insertions or deletions. Funding decisions may be predicated on requests for GOSIP-compliant equipment. Absence of such a request may be the basis for a bid protest.

Each agency may set up its own enforcement provisions, in addition to those described above. A decision should be made by each agency as to how to enforce GOSIP within that agency.

5.6 Specific GOSIP Applicability Recommendations

Specific recommendations that should be followed when determining whether GOSIP applies to a particular procurement are given below.

(1) Cost savings and GOSIP benefits over the long term should be considered in funding decisions for the current year. With the goal of increased interoperability and functional capability in mind, agencies should not sacrifice future capability for present cost effectiveness.

(2) Multi-vendor interoperability is an important reason for determining GOSIP applicability; however, GOSIP also applies to systems provided by a single vendor.

(3) Agency-specific procedures should be set up as soon as possible to handle waiver management and enforcement issues.

(4) Enforcement of GOSIP will largely be a local agency matter; agencies will have to "police" their own actions.

(5) Due to the benefits of GOSIP, it is expected that waivers will be granted only in exceptional cases.

(6) Configuration concerns should be identified.

5.7 Specific Concerns of Agencies

Even after reading section 5.2, questions may arise as to whether an agency's special requirements can be met by GOSIP. Each of the subsections below will address a particular category of user questions, in order for GOSIP applicability to be established.

5.7.1 Functionality

GOSIP should be used by Federal agencies when acquiring computer network products and services that provide equivalent functionality to the protocols defined in the GOSIP document; however, the functionality that is being procured need not be implemented in all hardware components. For example, a Message Handling System could be implemented on a mainframe with personal computers (PCs) providing terminal access using nonstandard software. Figure 7 gives an example of such an implementation.

GOSIP applies to new procurements or major upgrades of networking services specified in the GOSIP document. The question of what constitutes a major upgrade contains subjective elements which must be resolved at the Federal agency level in order to determine whether GOSIP compliance is required. This decision involves "gray" areas in which only general guidance can be given. The addition of a few nodes to a non-GOSIP electronic mail network will not force the agency to retrofit the Message Handling System specified in GOSIP to the entire network; however, a significant expansion of the network would require the agency to procure GOSIP-compliant products and to develop a method of interoperating with the existing mail system if a decision is made not to upgrade that system.

Some Federal agencies may be concerned that the functionality that they require is not in Version 2 of GOSIP. The GOSIP appendices contain a timetable for including additional applications and network services in GOSIP. Procurement authorities should use this information to determine whether it is appropriate to specify GOSIP in current procurements.

EXAMPLE: The Directory Services (DS) application will be in Version 3 of GOSIP, which is scheduled for release in 1992. In 1993, implementations conforming to the OSI international standards will be widely available and procurement of these implementations rather than vendor-specific or proprietary implementations will be mandated by GOSIP. If the DS implementation that is being procured in 1991 is not required until 1993, or if delivery is not expected until that time, then it is wise to require that vendors comply with the future GOSIP specification when it is mandated. Vendors that have a strategic commitment to OSI products will be able to provide this assurance.

5.7.2 Economic Considerations

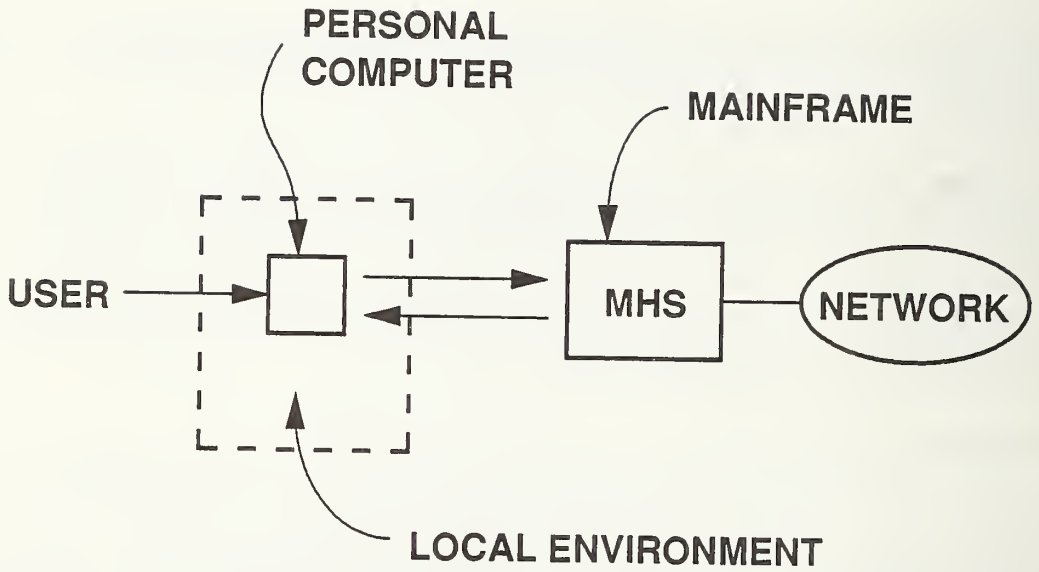
A question may be raised as to the cost of GOSIP products versus the cost of other choices. This is particularly relevant in light of total ADP budget constraints and limitations which are imposed currently on Federal agencies. The answer to this concern is that a major benefit of GOSIP is that it is expected to minimize total investment costs through extended life cycles, reduced conversion costs, and increased modularity. Thus, a smaller portion of ADP budgets will be required for purchase and installation of GOSIP technology than for purchase and installation of alternative equipment. Consequently, it is not anticipated that waivers will be requested for economic reasons. In other words, adoption of GOSIP makes good economic sense.

There is no minimum network configuration level specified for GOSIP compliance. Although the OSI protocols referenced in GOSIP are more viable and cost effective when many users and ADP systems are affected, the installation of these protocols is still economical on a per-unit basis even when interoperability is provided only to a few systems.

The initial costs of making the transition to the OSI protocols should not be a reason for GOSIP non compliance. There is a certain amount of overhead, training, and other agency effort required to change to any new technology. The initial cost of this short-term overhead should be greatly outweighed by the long-term cost savings resulting from the purchase and use of these protocols.

5.7.3 Research vs. Operational

A network may be judged as operational or research oriented. Some networks may be aimed at providing research into network function, protocols, or protocol performance. Such networks would not be bound by



MHS = MESSAGE HANDLING SYSTEM

FIGURE 7
MESSAGE HANDLING SYSTEMS
APPLICATION

GOSIP, because it does not make sense to apply a fixed protocol specification to networks investigating possibly varying protocol behavior or performance. Thus, waivers may be granted in this instance. An operational network is one that is oriented primarily toward providing reliable and efficient service to its users.

The term "network research" should not be confused with the term "research network." Network research involves research into networking technology. This does not imply that waivers are applicable for academic, scientific, or research networks.

It is a recommendation that each agency, using the above definitions and criteria, categorize each network as being operational or involved in network research. Most of the networks in the U.S. Government are operational because they offer basic day-to-day production capability; thus, GOSIP should apply to them.

6.0 GOSIP PROCUREMENT

6.1 Introduction

This section explains how to effectively procure GOSIP products. There is a general description of the procurement process and a discussion of procurement issues as they relate to GOSIP. In section 6.4, specific language will be suggested for users to include in solicitations. In section 6.6, technical evaluation issues, testing issues, and certification issues will be discussed. In section 6.7, vendor enhancements and acquisition strategies will be discussed. Finally will come an enumeration of different kinds of procurement scenarios; since every agency is different, this information is important.

This section will give specific recommendations on most procurement issues relating to GOSIP. For guidance on general procurement issues, readers should refer to their own contracting offices, to the General Services Administration (GSA), or to one of the appropriate references in the References section. Procurement actions referencing GOSIP are currently underway; an example is the Advanced Automation Systems contract developed by the Federal Aviation Administration.

GOSIP is an important document which may be used by both sophisticated and unsophisticated OSI procurement officials. The novice buyer may use the specific procurement language in section 6.4, and the more informed user may modify or add to this language to enable the creation and design of special-purpose applications and configurations in a flexible manner. Additional procurement-related information is given in sections 4.1 through 4.3 of the GOSIP FIPS.

6.2 OSI Procurement Summary

The general stages of an OSI procurement are as follows: (1) the determination by Federal management of a need for ADP equipment, (2) the need for the application user to identify specific requirements, (3) the need to determine whether GOSIP will meet these requirements, (4) the submission of requirements to procurement officials, (5) the determination by procurement officials of the appropriate method to use when creating and structuring the procurement documents, (6) the creation of the solicitation documents, (7) (possibly) an inquiry to prominent vendors as to what can be provided, (8) receipt of bids, (9) evaluation of bids, and (10) presentation of awards. Procurements of GOSIP-related ADP equipment will be bound by any relevant language contained in the FAR (Federal Acquisition Regulations) and/or FIRMR (Federal Information Resource Management Regulations).

In general, there is an order imposed on the above-described steps in the procurement process; in other words, one step must be completed before the next step can begin. The entire process may take a year or more to complete. The key step for OSI procurement is the writing of the solicitation document by the user; in particular, the way the requirements are written. This critically affects the outcome of the process. This requirements analysis should be as specific as possible, and be delivered to the procurement officials for formal preparation as procurement documents. It is anticipated that the basic procurement scenario, from the time that the detailed requirements analysis is received by the procurement officials to the actual award of the contract (Steps 4 through 10), will not change in the future because of any conditions pertinent to GOSIP.

It should be emphasized that GOSIP applies to new purchases only; existing contracts and acquisition cycles are not affected. Since the OSI technology is relatively new, it is incumbent upon users to familiarize themselves as quickly as possible with the OSI technology so that informed technical evaluation may be made over the life of an acquisitions process.

Table 1 gives the procurement steps most influenced by GOSIP, in decreasing order of importance, along with some recommended actions.

Table 1 – GOSIP Recommendations

STEP=3, NAME=Determine GOSIP Applicability, ACTION=See section 5

STEP=4, NAME=Submission of Requirements, ACTION=Produce Requirements Analysis

STEP=9, NAME=Evaluation of Bids, ACTION=See sections 6.6 and 7

STEP=7, NAME=Request for Information, ACTION= Draft RFP is Produced

6.3 GOSIP-Related Procurement Recommendations

Described below are aspects of OSI procurement that deserve special consideration by users planning to purchase OSI equipment. Adoption of recommendations stated herein should provide for a smoother OSI procurement process. The recommendations are enumerated below.

(1) In the case of OSI, it is recommended that Federal agencies pursue a competitive procurement strategy (open competition–selection not predetermined) along with a negotiated acquisition, if there are no other policy constraints. This is because the inherent philosophy of OSI is to enable choice among the best networking solutions available. A negotiated acquisition policy applied to selectee(s) will enable users to receive the maximum benefit in services provided.

(2) Agency officials should consider both present and future GOSIP functionality when making long-term procurement decisions.

(3) A draft purchase request is a preparatory document designed to elicit vendor comment; this is in advance of a formal purchase request. It is recommended that for OSI products, a draft RFP (request for proposals) be created. This is because it is important to determine what the vendors are able to provide; also, the OSI technology will be emerging in a series of steps or stages, and what can be provided next year may not be available this year.

(4) It is recommended that a clear, concise statement of work be developed for every planned OSI acquisition. This will reduce the number of questions asked of a solicitor by the vendors after an RFP is issued, and shorten the effective evaluation time.

(5) For OSI, it is likely that smaller vendors will "join forces" to submit bids in competition with larger vendors. This will enable all OSI vendors to compete in the market, and give the user many alternatives from which to choose. Users should be aware of this in their procurement planning.

(6) Since OSI is a new technology, agencies should consult with several vendors to determine a fair price; however, awards are expected to be made on technical merit as well as price.

(7) For OSI procurements, compliance to specified requirements must be accurately determined. Contractors responding to bids should be required to provide test certification from an authoritative source, or perform testing to demonstrate full compliance to the specified requirements. A GOSIP conformance and interoperation testing and registration policy [NIST 8] has been developed by the NIST. The goal of this policy is to provide Federal users with a list of GOSIP- compliant products.

(8) A list of customers who are using the OSI product should be required, if possible. The contractor should provide a plan for operational demonstration in the proposal. This plan shall delineate the methods by which the contractor intends to demonstrate to a U.S. agency how the proposed OSI product satisfies the stated OSI requirements. The agency will review this plan and ensure all requirements are tested and met.

(9) An acquisition plan should be developed for every OSI system under consideration by an agency for the next 10 years. Such a plan should include provisions for demonstration of source competence.

(10) OSI products might be available from standard GSA schedules, both independently and bundled with hardware. Federal users should investigate the GSA schedule option.

6.4 Particular "Contract Language" for RFPs

In previous subsections the general procurement considerations for GOSIP were given, and recommendations were made on issues pertinent to OSI. However, this is only meaningful if the user knows exactly what language to insert at the appropriate point in a solicitation document; recommendations will be given here, as well as guidelines for protocol selection and service interface definition. For more detailed guidance on these technical matters, the reader should refer to section 7 and to the Appendices.

It should be emphasized that (1) GOSIP specifies COMMUNICATIONS technology, and (2) GOSIP specifies functional requirements, not specific technical requirements in terms of particular ADP configurations (see sec. 5.3). Thus GOSIP deals with communications capability ONLY; all other ADP concerns are outside the scope of GOSIP. Also, GOSIP provides (1) reliable end system-to-end system service over different network technologies, and (2) applications that conform to international standards that use this reliable end-to-end service. Thus users are able to write special purpose applications conforming to (1) and (2) above.

EXAMPLE: An agency stores inventory data on magnetic tapes which are hand-carried from building to building. It is desired to replace this "system" by one using local-area network technology. GOSIP is certainly a candidate for consideration in this upgrade.

6.4.1 Determining Requirements

In general, the user should first determine what the application requirements are, and whether those requirements may be satisfied by GOSIP applications (file transfer, electronic mail, and remote login). There is a set of generic applications which is used in most Federal agencies. These include: basic file transfer, electronic mail, remote login, remote database access, electronic data interchange, and office document architecture. The user, in preparing a requirements specification for later solicitation, should examine the goals of the particular application or program, and look at the mechanisms or services by which these goals can be achieved. In other words, a user must determine functional requirements. If those functional requirements can be met by any of the GOSIP protocols, then compliance with GOSIP must be specified in future solicitations.

Factors in the above determination will be the length of the procurement process and the timetable for availablity of additional OSI functionality. It is important to remember that additional functionality reflecting user requirements will be added to future GOSIP versions.

It is possible for the user to have particular requirements for applications. The user needs to determine whether OSI products are consistent with and can support these requirements.

If this determination can be made, then products implementing the protocols contained in Version 1 of GOSIP must be specified in requests for proposals since GOSIP Version 1 FIPS was mandatory in August 1990. Products implementing the additional protocols contained in Version 2 of GOSIP must be referenced in solicitations beginning in 1992. If any other condition exists (e.g., the required functionality is not GOSIP-related, or there is a special architectural requirement), then a waiver may be requested. If granted, the user may specify alternative (non-OSI) solutions in solicitations.

In addition to application functional requirements, there are network technology requirements that must be considered by a user in a requirements analysis. As shown in figure 3.2 of the GOSIP FIPS, there are six alternatives; any of these is acceptable in a solicitation. Any of the GOSIP applications may reside "over" any of the network technologies. Similarly, the user must determine functional requirements for end-to-end transmission, and determine if the GOSIP-compliant technologies satisfy these requirements. For an existing system, it must be determined if specialized network technologies currently in use are able to apply GOSIP

technologies to satisfy functional requirements. If requirements can be satisfied, then one of the GOSIP network technologies must be chosen in a solicitation. If nonstandard network technologies are required, GOSIP may still prove useful for network interconnection, end-to-end transport, and applications. If any other condition exists, a waiver may be requestsd.

EXAMPLE: An agency has dissimilar Ethernets which use different physical media and are located in Florida, California, and Louisiana. These LANs are connected to mainframes which communicate using proprietary protocols over dedicated leased lines. It is desired to standardize LANs and upgrade to a single wide area network protocol (to save money). The GOSIP network technologies should be used.

6.4.2 Specific Language

NOTES

(1) THE GOSIP VERSION 1 FIPS (FIPS 146) CONTAINS REFERENCES TO SELECTED PORTIONS OF VERSION 1 OF THE NIST WORKSHOP AGREEMENTS. SINCE VERSION 3 OF THE NIST WORKSHOP AGREEMENTS IS NOW BEING REFERENCED BY GOSIP VERSION 1 (SEE SECTION 1.7, GOSIP VERSION 2), A SENTENCE SHOULD BE ADDED TO ALL QUOTED LANGUAGE AS FOLLOWS: "ANY NIST WORKSHOP AGREEMENTS REFERENCES IN FIPS 146 SHOULD BE REPLACED WITH UPDATED APPROPRIATE REFERENCES TO VERSION 3 OF THE NIST WORKSHOP AGREEMENTS."

(2) BECAUSE VERSION 3 OF THE NIST WORKSHOP AGREEMENTS IS MAINTAINED VIA AN ERRATA PROCESS (SEE SEC. 3), AND BECAUSE IT SHOULD BE THE RESPONSIBILITY OF VENDORS TO PROVIDE SUCH MAINTENANCE IN THEIR PRODUCT OFFERINGS, A SENTENCE SHOULD BE ADDED TO ALL QUOTED LANGUAGE AS FOLLOWS: "FUNCTIONALITY REFLECTING ANY ERRATA TO VERSION 3 OF THE NIST WORKSHOP AGREEMENTS WILL BE PROVIDED."

The procurement language below can be included directly in solicitations for purchasing the appropriate OSI products. The knowledgeable OSI user may modify or add to this language to suit individual requirements.

FTAM LANGUAGE

If a requirement exists for limited file transfer and management capability (such as that supplied by a print server), include language as follows:

"The product must conform to sections 4.2.5, 4.2.6, 4.2.7.1, and 4.2.7.2 of the Version 2 Technical Specification portion of FIPS 146-1. Specifically, FTAM functionality must be in accordance with section 4.2.7.2, ACSE functionality must be in accordance with section 4.2.7.1, Presentation Layer functionality must be in accordance with section 4.2.6, and Session Layer functionality must conform to section 4.2.5. For FTAM, Implementation Profiles T1 and M1 must be supported as stated in section 4.2.7.2. The product must be able to act in the FTAM role(s) of X."

In the above language "X" represents one or more of the allowable combinations of "initiator-sender," "initiator-receiver," "responder-sender," and "responder-receiver," as described in section 9.17 of the NIST Workshop Agreements [NIST 1]. See section 7.4.3 of this Guide for more information.

For greater file transfer, access, and management capabilities (such as those provided by a file server), use the language above with the replacement of "[T1 and M1]" by "[T2, M1, and A1]."

There may be instances where a system supporting limited capabilities as defined above may wish to retrieve sequential text files from a system with greater capabilities (as defined above). If this functionality is desired in a limited system, a sentence should be added to the language above (for a limited system) as

follows: "Simplification of FTAM-2 to FTAM-1 must be supported." See Appendix A and section 7 for more information on the above.

For further detail on above-mentioned capabilities, consult the NIST Workshop Agreements [NIST 1]. The coordination with vendors should be done before inserting the language in the paragraph above, because some early FTAM implementations may not have these enhanced capabilities. See section 6.5.1 of this Guide for additional procurement considerations.

MHS LANGUAGE

The terms "MHS" (for Message Handling Systems) and "X.400" are frequently used to refer to an application which allows users to send and receive messages over a store-and-forward message transfer system. If a requirement exists for electronic mail capability, include language as follows:

"The product must conform to sections 4.2.5 and 4.2.7.3 of the Version 2 Technical Specification portion of FIPS 146-1. Specifically, MHS functionality must be in accordance with section 4.2.7.3, and Session Layer functionality must be in accordance with section 4.2.5."

The solicitation must state whether Transport Class 0 is required, in addition to Transport Class 4 (see sec. 4.2.7.3 of the GOSIP FIPS). See section 6.5.2 of this Guide for additional procurement considerations. For more information on these CCITT Recommendations, refer to section 7.

VIRTUAL TERMINAL LANGUAGE

If a requirement exists to specify virtual terminal capability, include language as follows:

"The product must conform to section 4.2.7.4 of the Version 2 Technical Specification portion of FIPS 146-1, for system type Y."

In the above sentence, Y could be "simple system, "forms-capable system", or both. It is necessary for an agency to specify whether a simple system or forms- capable system is desired. Additional information in given in section 6.5.3.

NETWORK TECHNOLOGY LANGUAGE

If a requirement exists to specify a local area network with a CSMA/CD architecture, include language as follows:

"The product must conform to sections 4.2.1, 4.2.2, 4.2.3, and 4.2.4 of the Version 2 Technical Specification portion of FIPS 146-1. ISO 8802/3 shall be selected. In addition, intermediate systems must conform to section 4.3."

If a requirement exists for a local area network with a control access bus architecture, use the same language as above except replace "IS 8802/3" with "IS 8802/4." If a requirement exists for a local area network with a control access ring architecture, use the same language as above except replace "IS 8802/3" by "IS 8802/5."

If a requirement exists for an end system (ES) to intermediate system (IS) routing protocol, specify language as follows:

"The product must conform to section 4.2.3.1.2 of the Version 2 Technical Specification portion of FIPS 146-1."

Provision of the ES-IS functionality is as described in section 4.2.3.1.2 of the GOSIP FIPS. Additional information is given in section 7 of this Guide.

If a requirement exists for a network technology using wide area X.25 network facilities, specify language as follows:

"The product must conform to sections 4.2.1, 4.2.2, 4.2.3, and 4.2.4 of the Version 2 Technical Specification portion of FIPS 146-1. In addition, intermediate systems must conform to section 4.3."

If a requirement exists to integrate multiple network technologies into a GOSIP-compliant internetwork, specify language as follows:

"The product must integrate multiple network technologies (as described in sections 4.2.1 and 4.2.2 of the Version 2 Technical Specification portion of FIPS 146-1), in a manner prescribed by section 4.2.3 (plus subsections) of the above reference."

If a requirement exists to incorporate ISDN technology into an OSI network, use language as follows:

"The product must conform to section 4.2.3.4 of the Version 2 Technical specification portion of FIPS 146-1."

See section 6.5.5 of this Guide for additional procurement considerations.

TEST POLICY LANGUAGE

The NIST has issued GOSIP Version 1 testing guidance in "GOSIP Conformance and Interoperation Testing and Registration [NIST 8]. Federal agencies are advised to incorporate the following language into Requests for Procurement of products claiming compliance with the GOSIP Version 1 mandate:

"The AGENCY NAME requires that computer communications products for which GOSIP functionality is specified shall adhere to the provisions of the NIST GOSIP Testing Program as described in NISTIR 4594, 'GOSIP Conformance and Interoperation Testing and Registration.' In particular, GOSIP conformant products must appear on the 'Register of Conformance Tested GOSIP Products.' Interoperability must be demonstrated between different suppliers of GOSIP products, specified in this RFP, directly to this agency or by recording entries on a register indicated by the 'Interoperability Test Service' register."

A future revision to "GOSIP Conformance and Interoperation Testing and Registration" will add procedures, instructions, and recommendations for the new protocols included in GOSIP Version 2. Until this revision occurs, Federal agencies should use the interim guidance supplied in sections 2.1 and 2.2 of GOSIP Version 2.

For more information on the above, see section 6.6.5.

6.5 Optional Procurement Considerations

THE LANGUAGE IN SECTION 6.4.2 IS SUFFICIENT FOR GENERAL OSI PROCUREMENT. SPECIFICATION OF OPTIONS DESCRIBED BELOW REQUIRES TECHNICAL KNOWLEDGE.

AGENCY TECHNICAL OFFICIALS SHOULD BE PROPERLY INFORMED ON THESE MATTERS BEFORE THIS MATERIAL IS INCLUDED IN SOLICITATIONS. CONSULT SECTION 7 FOR ADDITIONAL INFORMATION

This section will list special options regarding procurement of File Transfer, Access, and Management (FTAM) products, MHS products, and Virtual Terminal products. Service interface definitions, network technologies, Presentation, Session, gateways, and some future procurement considerations are also mentioned. Products are expected to provide a variety of optional services and features. Appropriate language extensions will be given for each feature.

The Connection-Oriented Network Service (CONS) and the Connectionless Transport Protocol (CLTP)

are also included in Version 2 of GOSIP as options. Procurement language describing their inclusion is given in section 6.5.6.

6.5.1 FTAM (File Transfer, Access, and Management)

For FTAM there are the two broad classes of products desribed in section 6.4.2; one class offers limited file transfer and file management capability and the other offers greater file transfer, file access, and file management capability It is expected that there will be a variety of other options provided in FTAM products. Some of this functionality may not be available in the near future, but it will be made available eventually in response to user demand.

Several classes of options may be considered, and may be specified independently of one another. Such options describe additional capability to that offered in section 6.4.2. The categories are given below.

(1) Full file transfer allows reading to and writing from indexed files. To reference this, add a sentence to the "FTAM LANGUAGE" part of section 6.4.2 as follows: "Implementation Profile T3 as defined in the NIST Workshop Agreements must be supported." See section 9.19 of Version 3 of the NIST Workshop Agreements [NIST 1] for more information on T3.

(2) Full file access allows locating and erasing within indexed files. To reference this, add a sentence to the "FTAM LANGUAGE" part of section 6.4.2 as follows: "Implementation Profile A2 as defined in the NIST Workshop Agreements must be supported." See section 9.19 of Version 3 of the NIST Workshop Agreements [NIST 1] for more information on A2.

(3) File storage capability allows retrieval of complete information on file storage properties. To reference this, add the following sentence to the "FTAM LANGUAGE" part of section 6.4.2: "The storage group of FTAM attributes, as defined in ISO 8571-2 [ISO 3], should also be supported."

(4) File security capability (for banking systems) allows the retrieval of file security properties. To reference this, add the following sentence to the "FTAM LANGUAGE" part of section 6.4.2: "The security group of FTAM attributes, as defined in ISO 8571-2 [ISO 3], should also be supported."

(5) File directory capability is used for sending and receiving file directory information. To reference this, add the following sentence to the "FTAM LANGUAGE" part of section 6.4.2: "The document type NBS-9 as defined in the NIST Workshop Agreements must be supported."

(6) Office Document Architecture (ODA) capability. To include the capability of transferring documents formatted according to the ODA standard, add the following: "The FTAM-3 (ISO FTAM Unstructured Binary) document type must support the exchange of ODA information, as specified in section 4.2.8.1 of Version 2 of GOSIP."

6.5.2 Message Handling System (MHS) Options

In terms of MHS systems, the major components of a Message Handling System implementation are the Message Transfer Agent (MTA) and the co-operating User Agents (UAs). In addition to interacting with the Message Transfer System, the User Agents have many local functions which are outside the scope of international standardization, but not outside the scope of legitimate procurement concerns. These services include assisting the originator in creating and editing the message and in storing and presenting a delivered message to the recipient. These services will be provided in all User Agents, but any specific user requirements for these non-standardized services should be specified in the procurement request. A summary of some of the issues is given below; for more detail see the "MHS Evaluation Guidelines" [NIST 3].

Agencies that have the requirement to write their own nonstandard User Agents should specify a programmer-accessible interface between the User Agent and the Message Transfer System. If there is a requirement for a special-purpose User Agent, a sentence should be added to the MHS description in Section

6.4.2 as: "The User Agent shall provide the following capabilities:...," and then have these capabilities listed.

User requirements for the generation of optional Interpersonal User Agent elements should be specified. See section 7.4.2 and Appendix A for details. If it is desired to communicate over public messaging domains via public data networks, and an explicit service is required, add a sentence: "The product must be capable of communicating with CCITT-based public messaging systems."

The NIST Workshop Agreements have classes of MTAs to describe the MTA routing capabilities. Class 1 MTAs can route on country administration domain, private domain name, and organization name. Class 2 MTAs can also route on organizational unit. Class 3 MTAs can route on personal name in addition to all Class 2 attributes. Class 2 and Class 3 MTAs are GOSIP compliant. The routing tables required by Class 3 MTAs are more complex and Class 3 MTAs are not available from all vendors. Class 2 MTAs will provide all of the routing capability required by most users. Agencies should specify the requirement for either Class 2 or Class 3 MTAs in their procurement requests.

If there is a requirement to transfer documents formatted according to the ODA standard as the body part of an MHS message, then language should be included requiring the identification capability specified in section 4.2.8.1 of the GOSIP FIPS.

6.5.3 Virtual Terminal Options

To reference a simple VT system, add a sentence to the "VT LANGUAGE" part of section 6.4.2 as follows: "OIW VTE-Profile Telnet-1988 as defined in the NIST Workshop Agreements must be supported." See section 14.8.1 of the NIST Workshop Agreements for more information on the Telnet VT profile.

To reference a forms-capable VT system, add a sentence to the "VT LANGUAGE" part of section 6.4.2 as follows: "OIW VTE-Profile Forms-1989 as defined in the NIST Workshop Agreements must be supported." See section 14.8.3 of the NIST Workshop Agreements for more information on the Forms VT profile.

If an agency is procuring both a simple system and a forms-capable system, then a switch profile capability may be required (to move dynamically from one system to the other). In such an instance, appropriate language should be added to existing Virtual Terminal procurement language.

6.5.4 Office Document Architecture (ODA) Options

A Document Application Profile (DAP) specifies the constraints on document structure and content according to the rules of the ODA standard. Different DAPs can be created that apply to different classes of a document. Since DAPs are still in the process of being developed, Version 2 of GOSIP contains only the information required to transport any ODA document as the body part of a message or the content of a file. Future versions of GOSIP will reference applicable DAPs which the Computer Systems Laboratory of NIST plans to issue for Federal agency use.

6.5.5 Network Technology Options

The following applies to additions to the network technology language in section 6.4.2. The network technology choices are dependent upon the physical transmission capabilities employed. If compatibility with twisted-pair technology is required, then add the following sentence: "The Physical Layer must be compatible with twisted-pair media, as defined in 'X' " If coaxial cable is required, then add the following sentence: "The Physical Layer must be compatible with coaxial cable technology, as defined in 'X'." If fiber optic compatibility is required, then add the following sentence: "The Physical Layer must be compatible with fiber optics, as defined in 'X'." In the above sentences "X" is either ISO 8802/3, 8802/4, or 8802/5. If any other physical medium is required, add the sentence: "The OSI product must support the following physical medium:..., as specified in ...."

The transmission technique choices are: (1) for 8802/3 based systems, 10 BASE 5 or 10 BROAD 36, and (2) for 8802/4 based systems, 10 Mbps (broadband) or 5 Mbps (carrierband) (see NIST Workshop Agreements [NIST 1]). For (1) choosing 10 BASE 5 add: "The 10 BASE 5 CSMA/CD technology shall be supported, as defined in NIST Workshop Agreements [NIST 1]." For (1) choosing 10 BROAD 36 (for communication with 8802/4 broadband systems) add "The CSMA/CD 10 BROAD 36 technology will be supported, as defined in NIST Workshop Agreements [NIST 1]."

For (2) above, if choosing 10 Mbps broadband, add "For 8802/4 systems, the 10 Mbps broadband technology will be supported, as defined in NIST Workshop Agreements [NIST 1]." In choosing 5 Mbps baseband, add "For 8802/4 systems, the 5 Mbps baseband technology will be supported, as defined in NIST Workshop Agreements [NIST 1]."

There are several optional considerations for ISDN as well. For sending X.25 packet layer protocol data, insert the following sentence: "X.25 data will use ISDN via 'X'", where "X" is one or more of "D Channel (shared with signaling data)","B Channel (switched service)", or "B Channel (permanent service)." Consult section 2 of the NIST Workshop Agreements for more information on ISDN Physical Layer access.

If the Basic Rate Interface (BRI) is required for a system, include language as: "The BRI must be supported at X reference point(s)." In the above "X" is "S, T, or U", where "S" is the interface between the ISDN private branch exchange (PBX) and the ISDN terminals, "T" is the interface between the customer and the network terminating device, and "U" is the interface between the ISDN exchange in the carrier's office and the network terminating device.

If the Primary Rate Interface (PRI) is required, include language as: "The PRI must be supported at X reference point(s)." Here "X" is "S, T or U." There are a number of choices for B-Channel access capabilities. If one or more of the choices is required, add a sentence as:"The B-Channel access capabilities must be Y." Here Y may be any or six choices as follows: (1) circuit- switched access to a packet handler integral to an ISDN switch, (2) circuit- switched access to a packet handler separate from an ISDN switch, (3) circuit-switched access directly to another GOSIP end system or GOSIP intermediate system, (4) dedicated circuit access to a packet handler integral to an ISDN switch, (5) dedicated circuit access to a packet handler separate from an ISDN switch, and (6) dedicated circuit access to another GOSIP end system or GOSIP intermediate system.

6.5.6 CONS and CLTS

If a system requires the CONS (Connection-Oriented Network Service) as an option, insert language as:"The product must conform to sections 4.2.3.2 and 4.2.3 of the Version 2 Technical Specification portion of FIPS 146-1, in addition to section 4.2.3.1 of FIPS 146-1." If the CLTS (Connectionless Transport Service) is required, add language as: "The product must conform to section 4.2.4.2 of the Version 2 Technical Specification portion of FIPS 146-1, in addition to section 4.2.4.1 of FIPS 146-1."

6.5.7 Service Interface Choices

Users should state their functional and operational requirements in solicitations and leave the method of implementing those requirements to the vendors. Certain user requirements will cause vendors to supply a programmable service interface. These service interfaces constitute a "boundary" through which information flows from one OSI layer to an adjacent layer. Some common points at which programmable service interfaces may be provided by vendors are: (1) an Application Protocol (e.g., FTAM, MHS, Directory Services), and (2) a non-Application Protocol (e.g., a Transport or Session interface).

Defining specific interfaces for purposes of portability is a task beyond the resources of most users. Users with such requirements should support the development of standard interfaces to POSIX network services. In addition, requirements should be given to NIST personnel for input to the appropriate IEEE committees. Write to: Director, Computer Systems Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899 (ATTN: POSIX Networking Services).

6.5.8 Gateway Considerations

To incorporate OSI into an existing ADP environment, it may be necessary for technical or economic reasons to explicitly require a gateway in a solicitation. Such a gateway would convert information in a vendor-specific or proprietary protocol to equivalent information in the OSI protocol and vice versa. If this action is necessary, add a sentence to any of the paragraphs in section 6.4 stating: "An OSI gateway must be able to completely and effectively convert between [A and B], and the vendor must document impacts on services and protocols provided by the gateway." Here, "A" is a vendor-proprietary protocol, and "B" is the equivalent OSI protocol(s).

Quite often, vendors will provide gateway capability as described above as a largely transparent "value-added" service. Users should discuss such possibilities with vendors as part of the acquisition process.

6.5.9 Presentation and Session

The NIST Workshop Agreements require that the Presentation kernel functional unit be supported. This supports the services required to establish a Presentation connection, transfer normal data, and release a Presentation connection. The Application Layer protocols determine the Session layer functional units needed for their support. For an explanation of the above-mentioned capabilities, refer to section 7. In general, any Presentation and Session services outside those required to support specific applications must be specified by the user. Such extra services are not likely to be available.

6.5.10 Future Considerations

Additional OSI protocols and services are expected to be available within the next few years. Specific procurement language will be given when these protocols and services are included in a future version of the GOSIP FIPS. For additional information on this ongoing work, refer to section 7 of this Guide and to the appendices to the GOSIP FIPS.

6.6 Evaluation Process for Procurement

Technical details necessary for proper evaluation are described in section 7 and Appendix A of this document. Federal users should solicit appropriate technical individuals to analyze their requirements. It is extremely important that evaluation responsibilities be assigned only to individuals that have an understanding of system specifications, system requirements, acquisition regulations, and contract administration.

The recommended OSI evaluation process steps are: 1) define and document user requirements, 2) study technical information contained in vendor product announcements, 3) evaluate which implementations, among several candidates, best meets the user's functional and performance requirements, 4) make selection from the Register of Conformance Tested GOSIP Products, and 5) provide complete documentation to those who were not selected. For more information on the GOSIP test policy, refer to section 6.6.5.

NIST has recently published "Guidelines for the Evaluation of Message Handling Systems Implementations" [NIST 3] This document can assist evaluation authorities in determining which MHS implementation best meets their requirement(s). An algorithm is provided to assist in the rating process. Guidelines for evaluating FTAM implementations will be published in 1991; guidelines for evaluating implementations of other OSI applications (e.g., Directory Services, Virtual Terminal) are expected in the future.

The contracting officer's review of nontechnical OSI factors will generally be divided into two phases: (1) a review of the business aspects of the bid or offer, and (2) a business review of the contractor's operations and qualifications. It is recommended that the organizational unit initiating the procurement not be made aware of the proposed prices. This is to ensure that technical evaluations are based solely on technical factors.

The negotiation method should be used with all large purchases; for small purchases a straight "low

bid" approach may be taken; this is particularly true for "generic" OSI technology. Furthermore, since OSI products are in an early phase of development, it is recommended that Federal agencies negotiate with the most highly-qualified vendors to obtain the maximum OSI functionality desired, even if the cost is not minimal. Selection should be based on functionality supplied, not cost alone.

An extensive set of benchmark tests may be required in a RFP; these tests should span the entire range of capabilities required by a system. Demonstrations should be mandated for each vendor. These benchmarks should be fair and open and should not bias one vendor in favor of another. Technical experts at each agency will identify critical and noncritical OSI product capabilities to be tested.

For proper and complete evaluation of GOSIP products, since OSI technology is new, it is recommended that a review of at least 3 months be undertaken for all commercially available OSI products. This recommendation is waived when: (1) minor OSI components are being considered, and (2) in the future, when bids are received from contractors who have previously produced identical OSI products for the Government.

6.6.1 Conformance Testing

Conformance testing verifies that a protocol implementation performs as the standard specifies. Most conformance test scenarios concentrate on single layer testing. A single layer of the OSI protocol stack is tested using the services of the lower layers which have been tested previously and are, therefore, assumed to be correct.

Conformance testing alone will not ensure that an OSI protocol suite will work correctly. No conformance test system can ensure that all errors in a protocol implementation will be detected. In addition, single layer conformance testing is not always possible, because some vendors merge the functionality of two or more layers in a protocol implementation. However, conformance testing will increase significantly the probability that a product interoperates with other products.

6.6.2 Interoperability Testing

Interoperability testing simulates the "real-life" conditions under which the vendor's product will be seen. Since vendors of OSI products are building implementations to operate with implementations developed by other vendors, it is in both the customer's and vendor's interest to duplicate as closely as possible the environment in which the product will be used before product acceptance is completed. In general, interoperability testing detects configuration options that are set in an incompatible manner. Such errors are relatively easy to overcome.

6.6.3 Performance Testing

Federal agencies may compare performance data, produced by vendors or research organizations, against agency requirements. The NIST may provide advice on realistic performance requirements given certain technological considerations. In addition, users need to determine the performance requirements pertinent to their particular situation. The NIST is developing performance metrics and benchmarks for certain GOSIP applications. Such a document for the MHS application is now available [NIST 3].

6.6.4 Functional Testing

GOSIP mandates, for each protocol, a minimum set of functions to meet general government requirements. In many instances, additional functions might be supported within the NIST Workshop Agreements and/or the protocol standard. An agency must determine and specify whatever additional functions are required in a solicitation. An agency should also ensure that the vendor products proposed meet all functional requirements of that agency, regardless of whether or not those additional functions are subject to standardization.

6.6.5 GOSIP Testing Policy

The GOSIP FIPS requires Federal government agencies, when acquiring computer network products and services, to procure OSI products, as specified in GOSIP. A companion FIPS, GOSIP Conformance and Interoperation Testing and Registration [NIST 8], places certain responsibilities on GOSIP product suppliers and makes recommendations to agencies. A tutorial document [NIST 11] gives a synopsis of the same information. A summary follows.

The "GOSIP Conformance and Interoperation Testing and Registration" establishes the framework by which Federal agencies can ensure that procured GOSIP products are compliant with the GOSIP specifications. The vehicle by which this determination can be made is a set of registers, published periodically by NIST. These include registers for test suites, test systems (means of testing), conformance testing laboratories, and interoperability testing services. However, the single register of most use for agency procurement purposes is the Register of Conformance Tested GOSIP Products. Products successfully tested in an accredited testing laboratory against a registered means of testing may be entered onto that register.

The complete list of registers is: 1) GOSIP Abstract Test Suites, 2) Interoperability Test Suites, 3) Assessed Means of Testing, 4) NVLAP Accredited Test Laboratories, 5) Conformance Tested GOSIP Products, 6) Interoperable GOSIP Products, and 7) Interoperability Testing Services. Entries on each of these registers are described in the "GOSIP Registration Criteria" handbook [NIST 12].

In order for a Federal agency to ensure that products are effectively tested to establish GOSIP compliance, the following criteria hold:

1) GOSIP shall be used by Federal Government Agencies when acquiring computer network products and services (and communications systems or services) that provide equivalent functionality to the protocols defined in the GOSIP FIPS 146 and referenced standards.

2) If a supplier CLAIMS GOSIP compliance or conformance for a product, then the agency is advised to require that product to be tested in accordance with the criteria specified in the GOSIP Conformance and Interoperation Testing and Registration Report. If the product includes a multi-layered GOSIP profile then ALL protocols for which GOSIP compliance or conformance is claimed should be tested in accordance with these criteria.

3) Federal Government Agencies requiring verification of supplier's claims of GOSIP conformance should consult the Register of Conformance Tested GOSIP Products.

4) Federal Government Agencies wishing to procure OSI products that are not on the register are advised to arrange that the product qualify for registration prior to final acceptance.

5) Federal Government Agencies should consult the data supplied by a service on the register of Interoperability Test and Registration Services under any of these conditions: (a) the agency requires that multiple instances of successful interoperation are documented for a specific GOSIP-conformant product, and b) the agency requires that an instance of successful interoperation is documented for one or more specific pairs of GOSIP-conformant products.

Using procedures developed by the Computer Systems Laboratory and the National Voluntary Laboratory Accreditation Program (NVLAP), the NIST will evalutate and accredit the abstract test suites, means of testing (i.e., test systems), and the test laboratories that can be used to certify GOSIP conformance. An initial set of laboratories accredited to perform conformance testing for GOSIP Version 1 protocols was identified by the end of 1990. Agencies may request statements that certify successful completion of testing from the vendors or test laboratories. Agencies may also consult a list of GOSIP-compliant products to be published quarterly by NIST.

Until such time as abstract test suites, means of testing, and test laboratories are accredited to perform conformance testing for the additional protocols in Version 2 of GOSIP, Federal agency authorities shall be responsible for determining the test systems and test cases required for conformance to GOSIP Version 2.

They shall also determine minimum acceptable test results for the purposes of procurement. Acquisition authorities may consult with the NIST to assist in this process.

The NIST will also evaluate candidate OSI interoperability testing services. Successful candidates, to be identified on a publicly accessible register, must: (1) be an organization recognized by NIST, (2) use an interoperability test suite recognized by NIST, (3) arrange for a bi-lateral test agreement between pairs of GOSIP product suppliers, (4) select a common subset of tests including the mandatory tests for GOSIP, (5) provide a joint declaration from each pair of test partners for each successful test campaign, and (6) make available, upon request, to NIST a copy of the detailed test results for any specific test campaign. NIST has published interoperability tests for MHS [NIST 9] and FTAM [NIST 10] that were developed by OSINET, an informal group of OSI suppliers and users, and subsequently coordinated among other similar groups aggregated under the name OSIone. For further information, consult the GOSIP Conformance and Interoperation Testing and Registration FIPS [NIST 8].

6.7 Vendor Enhancements and Acquisition Strategies

If agencies have particular needs that may not be satisfied by current OSI standard products, then they may request and respond favorably to enhancements containing these nonstandard or interim services. As a part of a vendor response, a transition plan should be included indicating how these nonstandard services will evolve to standard OSI solutions in the future. Care should be taken to ensure that nonstandard enhancements do not compromise basic interoperability.

Several examples are apparent, in the form of directory service enhancements and network management solutions. In either case, vendors may offer interim solutions as enhancements to OSI products, in the absence of standards supporting these capabilities. Interim specifications (i.e., MAP/TOP Network Management Building Block) may be proposed as a short-term solution. Users may wish to accept these options, and require that the vendor propose a transition path to the standard OSI solutions when they become available in products.

Another example is that of security enhancements to OSI products. Many users have security needs that must be added as options to existing OSI products. Comprehensive security standards are not available currently. Users may accept interim security solutions, if needs exist. These solutions should be moved to OSI solutions in the future, and it is recommended that vendors provide a plan or specific commitment for such a transition.

Vendors may upgrade their products to align with evolving base standards or functional profiles, or they may provide additional functionality beyond that contained in GOSIP. In these instances, care should be taken that full interoperability of these products with other GOSIP-compliant products not be compromised.

6.8 Specific Examples of Procurement

Each agency will find itself with different procurement concerns, because the characteristics of each agency are different. Each agency has its own set of system life cycle and configuration decisions to make; these will be more fully explored in section 9. This fact will affect the procurement decisions that must be made. Some general procurement-related scenarios may be defined. It is likely that an agency will find itself in one of these procurement scenarios.

The first procurement scenario is one in which all procurement efforts are contracted out (and then given to subcontractors). In this situation the Federal official should interact frequently with non-Federal contractors to ensure that the wishes of the Federal officials are being met in the contracting process. This includes specifying when and how benchmarking tests are to be run, specifying application performance requirements, and monitoring the life cycle of the contract, including when and how the contract money is to be spent. This is particularly critical in the area of system upgrades.

A second procurement scenario is one where there are a number of large pre-existing proprietary networks

that will be extant for the next few years. The stated purpose of OSI products will be to interconnect existing networks and maintain existing applications. A procurement strategy here would be to specify OSI gateways, routers, or possibly dual protocol suites. For more information on gateways, dual suites, and routers, consult section 9.

A third procurement scenario is one where system upgrades occur; that is, additional OSI capability will be developed, and major additional OSI hardware and software purchases will be contemplated. However, this expansion is entirely under the control of one central authority. As system life cycles expire, replacement will occur with OSI technology. The strategy here is to develop at the outset a comprehensive long-term acquisition plan which will describe progress at a steady pace toward a complete OSI environment at some specified time in the future. Key dates should be identified when specified "levels" of OSI functionality should be achieved. Gateways may be procured as part of a transition strategy.

The fourth procurement scenario is similar to the third, but in this case, there are many different centers of administrative and technical control. Different components of an agency may be at different stages in OSI evolution, and close cooperation must be maintained with the regional centers to move towards an integrated OSI environment as soon as possible. The procurement strategy here is for each center of authority to develop an acquisition plan for its environment, and for there to be a series of meetings to coordinate progress towards OSI. Each center of control should not be "bound" or "restricted" by the nature of acquisition strategies at other centers. There should be an effort to embody all of the possible procurement strategies in a comprehensive transition plan for the entire agency.

An agency should determine which of the above scenarios applies, and take the indicated actions. Table 2 summarizes the example generic procurement scenarios depicted, and the appropriate actions in each case.

Table 2 – Procurement Scenarios

CATEGORY=Contracted Out, STRATEGY=Contractor Monitoring

CATEGORY=Connecting Networks, STRATEGY=OSI Gateways and Dual Suites

CATEGORY=System Upgrade (Centralized), STRATEGY=Centralized Acquisition Plan

CATEGORY=System Upgrade (Distributed), STRATEGY=Distributed Acquisition Plans

CATEGORY=System Upgrade (Distributed), STRATEGY=Overall Transition Strategy

7.0 TECHNICAL ISSUES

7.1 Introduction

This section provides supporting technical documentation necessary to perform proper evaluation of vendor proposals as described in the previous section. The user will need to understand this material in order to interpret product announcements. After reading this section a user should have a greater awareness of the technical capabilities of OSI products. The Federal technical specialist evaluating GOSIP products must be aware of the technical issues to be considered at the time the evaluation is made. The specialist after completing this section should have a greater understanding of OSI concepts.

This section gives (1) a summary of the OSI Model, (2) a synopsis of technical considerations in three areas (protocol, service interface, performance), (3) guidelines for evaluating information in product announcements, and (4) some examples of OSI information flow. For an evaluation of technical considerations, readers should refer to subsections 7.3 and 7.4. For an interpretation of product announcement information, readers should refer to subsection 7.5. For examples of OSI scenarios, readers should refer to section 7.6. Descriptions of future work planned for inclusion in GOSIP are given in section 7.7. For additional, tutorial material, refer to Appendix A, and for standards references, refer to Appendix B.

7.2 OSI Reference Model Summary

The OSI standards were developed to allow computer systems built by different vendors to exchange data. Even though these computer systems have different operating systems and vary in how data is processed internally, as long as the information that passes between the processors conforms to the OSI international standards, information can be interpreted upon receipt and communication is possible.

The first step in OSI standards development was the creation of an OSI Reference Model [ISO 1]. This model, developed by the International Standards Organization (ISO), is divided into seven layers; each layer provides a well-defined set of functions necessary for the effective transmission of data. Each of these layers provides a service to the layer above by carrying on a conversation with the same layer on another processor. The rules and conventions of that conversation are called a protocol. At each layer N, there is an N-layer protocol. The information that is passed between a layer on one processor and the corresponding layer (or peer entity) on another processor is called a protocol data unit.

Service primitives are special messages which define the services that a layer provides. The details of how the services are implemented are transparent to the service user, usually the next upper layer. Communication between layers is via a service access point, or a special location through which service primitives pass. Service request and service response information passes between adjacent layers at the service access point.

Brief descriptions of the services provided by each of the seven layers of the model are given in the GOSIP FIPS. The important principles are that (1) each layer performs a unique, generic, well-defined function, and (2) layer boundaries are designed so that the amount of information flowing between any two adjacent layers is minimized. A particular layer has to provide a sufficient number of services to the layer immediately above for that layer immediately above to properly perform its functions. The ISO/IEC international standards (ISs) and CCITT recommendations are based upon the same Reference Model, shown in figure 8.

The functions of each of the protocol layers will be explained later in this section. The protocols can be connection-oriented or connectionless. In connection-oriented protocols, a user must set up a virtual connection, which is valid for the life of the communications activity, and disappears when the communications activity disappears. The converse of this is connectionless activity, whereby the user does not set up a virtual connection but communicates by transmitting individual "pieces" of information. An example of the former is a telephone conversation; an example of the latter is message delivery by the postal service.

The relationship of the protocols in the layers of the OSI model has been compared to a "wine glass." A

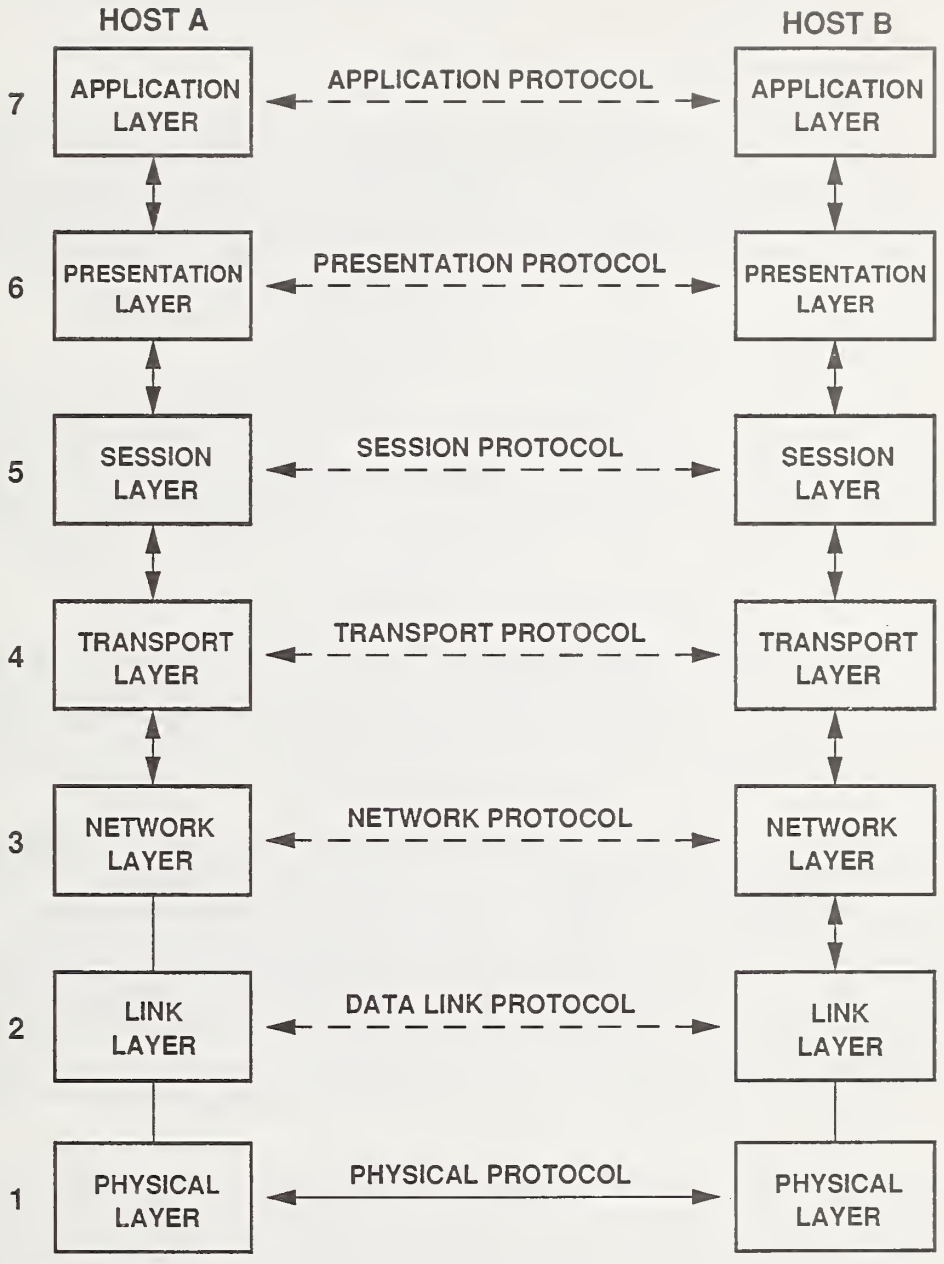


FIGURE 8
ISO REFERENCE MODEL FOR OSI

number of user applications are defined (top of the glass). Each of these may have slightly different means of support from the functional layers (sides of the glass). All applications have reliable end-to-end service provided via the Transport Layer and Connectionless Network Protocol (stem of the glass). This is the "glue" that holds the top and bottom together. At the bottom are the various network technologies (base of the glass). Figure 9 illustrates this.

7.3 Protocol Considerations

Based on the general information given above, the functional capabilities of each of the protocols referenced in the GOSIP FIPS are described below. The discussion includes a description of capabilities provided by the protocol (to assist the user) and, where applicable, options as to how the protocol might be implemented. It should be a vendor decision as to how to implement OSI protocols, but users should have a general knowledge of possibilities so that they can evaluate vendor offerings and can make special requests, if necessary.

7.3.1 Association Control Service Element (ACSE) Protocol

ACSEs provide common association or connection control services that are needed by a number of applications; it is more efficient to incorporate these services into a common protocol than to reproduce them, perhaps differently, in every application. The ACSE protocol performs essential services for the application, such as connection establishment, connection release, and error notification. An everyday example is a telephone conversation, where a secretary establishes a telephone connection for a manager.

7.3.2 File Transfer, Access and Management (FTAM) Protocol

"FTAM" in GOSIP describes the File Transfer, Access, and Management (FTAM) Standard. This standard provides a means of communicating about groups of related information, i.e., files. A user can move files, interrogate the properties of files, and manipulate files on a variety of different systems, without knowledge of the characteristics of any particular file system. This is accomplished by means of a common communications model and language, as described in the standard.

Services of FTAM provided to the applications user are: (1) the ability to communicate about files without specific knowledge of the other system's file characteristics, (2) the ability to express exactly what the user requires, and (3) the ability to include detailed transfer, access and management mechanisms.

FTAM describes a two-party interaction between an initiator and a responder that reacts to the initiator's requests in a passive role. Steps in a typical FTAM activity are to: (1) establish an FTAM association with a recipient, (2) select a file, (3) modify the properties of that file, (4) open that file, and (5) perform data transfer on that file. FTAM allows one to access and transfer an arbitrary number of different file types, and allows detailed (record-level) access to any one type where appropriate. For more details on FTAM, consult Appendix A.

Two categories of FTAM systems are defined by GOSIP for procurement purposes: (1) limited-purpose systems, and (2) full-purpose systems. A limited-purpose FTAM system provides the functions of simple file transfer and management. A full-purpose FTAM system provides the functions of positional file transfer (including simple file transfer), simple file access, and management. A limited-purpose FTAM system is able to interoperate with a full-purpose FTAM system at the intersection of their capabilities. An extra consideration is added for limited-purpose systems wishing to retrieve sequential text files from full-purpose systems (see sec. 6.4.2).

7.3.3 Message Handling Systems

The Message Handling Systems application is based on the CCITT X.400 Series of Recommendations. These Recommendations specify a store-and-forward Message Transfer System consisting of individual Message Transfer Agents which cooperate to deliver a message from Interpersonal User Agents serving an origi-

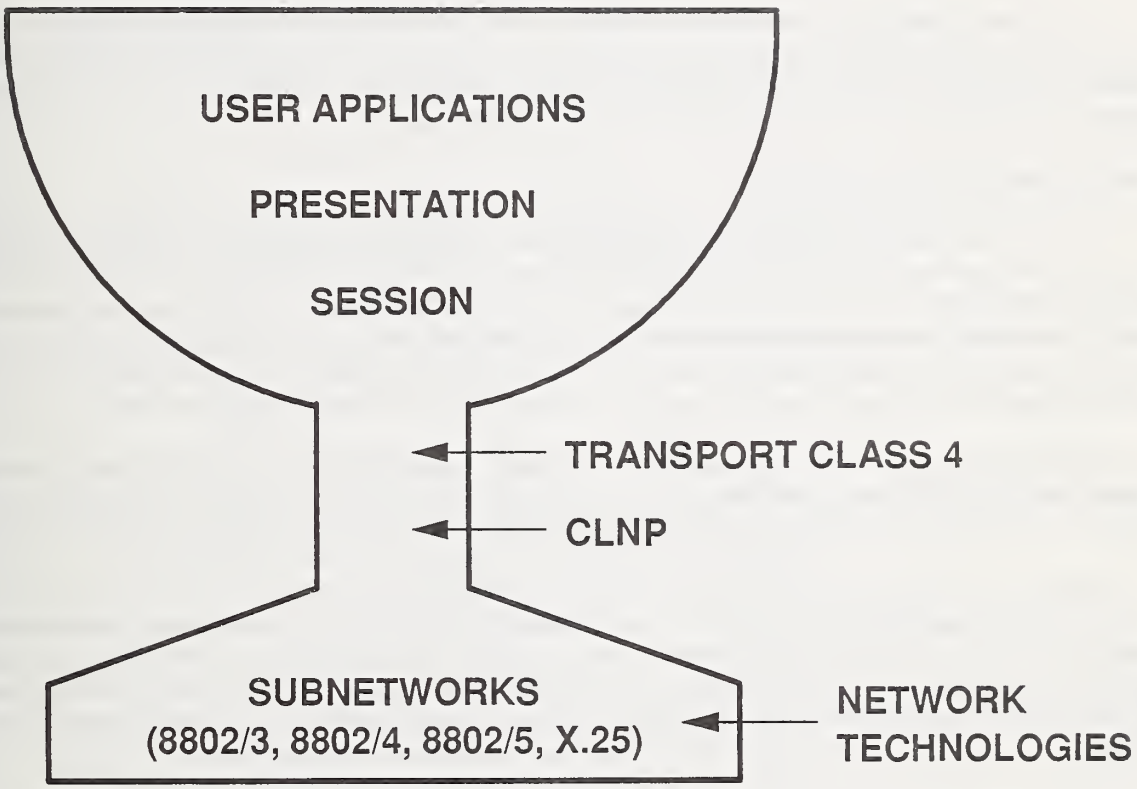


FIGURE 9
OSI "WINE GLASS" EXAMPLE

nator to Interpersonal User Agents serving one or more recipients.

An analogy is that of a user writing a letter (message), inserting it into an envelope, and delivering it to a post office. Envelope and contents are routed to a destination post office via intermediate post offices (possibly); once at the destination, that post office delivers the letter to the recipient's home. The destination User Agent is the recipient's mailbox; the post offices are Message Transfer Agents.

The Message Transfer System, like the post office, provides special services such as delivery and non-delivery notifications, priority delivery, and deferred delivery. The User Agents which submit messages to and receive messages from the Message Transfer System can be under the same management as the Message Transfer System, or they can be under separate management.

A message consists of an envelope and contents. The envelope contains address information, and the contents may contain different encoded information types. In sum, the MHS provides an efficient means of transmitting messages from an originator to one or more recipients. See Appendix A for more details on the MHS.

7.3.4 Virtual Terminal Protocol

The Virtual Terminal Protocol allows terminals and hosts to be on different networks in order to have an interactive conversation without the remote host having knowledge of specific terminal characteristics. The terminal characteristics are generally defined in a virtual terminal which is known or agreed between VT users. The generic, network terminal characteristics are mapped onto specific, local terminal characteristics before information is displayed on the terminal. The process is reversed upon terminal input; specific, local terminal inputs are mapped to generic, network terminal inputs for transfer across a network.

Communication between two general terminal types is provided by the Virtual Terminal protocol in Version 2 of GOSIP. The two categories of VT systems defined are: 1) simple systems, and 2) forms capable systems. A Federal agency may procure the VT protocol for either or both of these systems.

Both kinds of systems serve character-based user interaction, but they differ in the extent to which the system at the terminal end can process the user's input. The simple system can perform limited editing of user input, at most one line at a time, and can also support a transparent mode in which each character is passed to the application end for processing. The forms-capable system provides the application end with the capability to define fields on the terminal end system, where each field can be defined with specific data entry instructions which are then used by the terminal end system to process the user's input.

These systems are independent, in that one is not a subset of the other. In specifying a VT system, these two types of systems are distinguished by the VT profile supported.

A simple system provides the functions af a TTY-compatible device. The dialogue is line-at-a-time or character-at-a-time A simple system uses the control character (single) functions from the ASCII character set, such as "carriage return" and "form feed." A simple system must support the TELNET profile from the NIST Workshop Agreements.

A forms-capable system is intended to support forms-based applications with local entry and validation of data by the terminal system: functions such as "cursor movement," "erase screen," and "field protection." A forms-capable system must support the forms profile as defined in the NIST Workshop Agreements.

The Telnet and Forms VT profiles define two very different levels of service. The Telnet profile can be used to provide network login for a terminal user wishing to interact with a command line interpreter or one of the many character-based applications in existence today. The Forms profile provides an environment for the development of field-oriented applications, wherein the application defines the fields, the data entry rules, the navigation path linking the fields together and actions to be taken when field entry instructions are violated, while the system serving the terminal end of the dialogue enforces the field entry rules and

follows the actions prescribed by the application.

7.3.5 ODA

Office Document Architecture (ODA) is not an OSI ptotocol; it is an interchange format that provides for interchange of documents (including text, facsimile and graphics information) which are produced in an office environment. It is referenced in GOSIP because GOSIP applications (MHS and/or FTAM) may be used to convey ODA information between two users. Furthermore, agreements are needed in both the NIST/OSI Workshop and in the GOSIP FIPS to provide for this transfer. Federal agencies should ensure that these specifications are referenced in procurement requests, if ODA document transfer is required within either electronic mail messages or files.

7.3.6 Presentation Layer

The services of the Presentation Layer are specified in IS 8822 [ISO 11]. The Presentation Layer deals with generic functions that are needed by many different kinds of applications; specifically, a common means is provided of representing a data structure in transit from one end system to another. It is necessary that each side of the transfer understand the content and meaning of what is being transferred. Accordingly, the Presentation Layer will take information from the applications, and convert this information into a form and structure that can be recognized and interpreted by the destination OSI end system.

Basic functions performed at this layer include: (1) data representation functions (as described above), and (2) connection-oriented functions. Representation deals with the way the actual data is coded or represented during data transfer. Connection functions deal with establishing, preserving, and managing the connection between two applications.

An example of the function of the Presentation Layer is indicated by the following: a Frenchman speaks French and German, and an American speaks English and German. The Presentation Layer provides the means for the two parties to recognize that they need to have their conversation in German. The Presentation Layer would convert both languages to German for communication purposes.

Presentation is described in terms of functional units, or groupings of similar functionality; these are the kernel, context management, and context restoration. The kernel refers to the connection-oriented matters mentioned above. Context management refers to defining and manipulating the format (context) of information, and context restoration refers to retrieving a context that may have been used previously. For end systems, there is sender-Presentation code and receiver-Presentation code. In sum, Presentation allows any type of system to understand information provided by any other type of system by conversion to a common information format.

The Presentation functional unit needed to support FTAM and VT is the kernel functional unit. There is no explicit Presentation Layer required for the MHS mail protocol standardized in the 1984 CCITT Recommendations; the functionality is incorporated in the Application Layer.

7.3.7 Session Layer

The Session Layer provides user-oriented services to aid in the orderly and reliable flow of information between users in two different end systems. These services provide for increased efficiency in managing the dialogue between applications. Some functions provided by the Session Layer are synchronization (setting and resetting positions of data at each end of the connection so that each side knows where to start), and checkpointing (marking the data for convenient reference). The Session Layer protects applications and users from irregularities and problems in the underlying network.

The Session Layer protocol is also organized in terms of functional units; examples of these functional units are kernel (basic connection and data transfer) and duplex. Also included are half-duplex, expedited data, minor synchronize, major synchronize, typed data, activity management, resynchronize, and excep-

tions. For a further explanation of these, consult the reference under "ISO-Session Layer" in Appendix B.

There are two types of dialogue control. Either end can send data at any time (duplex) or each end can take turns sending data (half duplex). In the latter case, tokens are used to control the direction of data transfer and which process is authorized to send data. Data may be synchronized, which allows retransmission to start at a convenient point; data may also be expedited, which means that it has a higher transmission priority. Data may be typed, which allows it to be sent even if the sender does not possess the token.

FTAM and MHS have different Session requirements and options. For FTAM, the required Session functional units are kernel and duplex, and the optional functional units are resynchronize and minor synchronize. For the MHS application, the required Session functional units are kernel, half-duplex, exceptions, activity management, and minor synchronize functional units. For the VT application, the Session functional units required are kernel, duplex, expedited data, major synchronization, resynchronize, and typed data.

7.3.8 Transport Layer

There are two types of service available from the Transport Layer as follows: (1) connection-oriented, and (2) connectionless. Each is supported by a separate and distinct protocol and is used in different circumstances.

7.3.8.1 Connection-Oriented Transport Protocol

A pre-fabricated house is moved piece by piece from one state to a new state and reassembled properly with no damage having been done in transit. This is what the Transport connection-oriented protocol does with data between two end systems. The protocol provides reliable, orderly end-to-end data transfer. This means that data packets are received uncorrupted and in the correct order by the Transport Layer user. The basic function of connection-oriented Transport is to provide the difference between the quality of service desired by the Transport Layer user and that which is provided by the Network Layer (see sec. 7.3.9).

There are many parameters that are negotiated between two communicating Transport entities. These provide for proper flow control, proper sequencing, and proper error detection and retransmission of lost data. The international standard contains provisions for five classes of Transport service (Class 0 through Class 4). Class 4 assumes the least about Network Layer services, and is required for GOSIP systems. Class 0 is also required in certain circumstances (see sec. 4.2.7.3 of the GOSIP FIPS).

7.3.8.2 Connectionless Transport Protocol (CLTP)

The Connectionless Transport Protocol (CLTP) is used to provide the Connectionless Transport Service (CLTS). The CLTP is to be used only as an option among participants with a similar capability. There currently are no detailed implementation agreements from the NIST/OSI Workshop for connectionless protocols at OSI layers above the Transport Layer. Thus, the Connectionless Transport Protocol is included so that non- OSI applications can take advantage of its services. For example, it is possible to run non-OSI applications, such as the Network File System (NFS), using the CLTS. The Connection-Oriented Transport Protocol (COTP) is still the only protocol that provides reliable end-to-end communication between GOSIP-compliant systems.

7.3.9 Network Layer

There are two types of service available from the Network Layer – Connection-Oriented and Connectionless. The function of the Network Layer is to relay and route network service user packets to the correct destination, while at the same time masking the differences in the underlying subnetwork technologies (e.g., X.25 and CSMA/CD). The source and destination network service users may be on the same subnetwork or different, interconnected subnetworks.

7.3.9.1 Connectionless Network Service (CLNS)

The Connectionless Network Service (CLNS) is provided by the Connectionless Network Protocol (CLNP), which allows different subnetwork technologies, as referenced in GOSIP, to be interconnected. These include local area networks 8802/3 (CSMA/CD), 8802/4 (token bus), and 8802/5 (token ring) as well as X.25 and ISDN subnetworks. The CLNP masks the differences between these subnetwork technologies and allows these differences to be transparent to the OSI Network Layer user.

The services of the existing subnetwork technologies must be augmented to provide the OSI Network Layer service; this enhancement is also provided in the CLNP. Since the protocol to provide this service is connectionless, each protocol data unit is routed separately and the header of each protocol data unit contains addressing information as well as information relating to optional services provided by the protocol (e.g., priority and security). Work is in progress to allow the CLNP and the Connection-Oriented Network Service (CONS) to interoperate or interwork; some of the suggested methods are discussed in section 9.

The GOSIP FIPS specifies a pertinent network addressing structure. Other network addressing structures (e.g., wide-area network (WAN)-oriented addressing structures) may be appropriate in some architectures and these addressing structures are not out of alignment with the OSI IS-IS routing protocol currently under development (see sec. 7.7.6), though they may not be optimal.

Version 1 of GOSIP originally required that the processing of Protocol Data Units by the CLNP be in order of priority. That requirement has been deleted in an addendum to GOSIP Version 1, since under certain circumstances this could significantly decrease throughput in intermediate systems.

The End System (ES) - Intermediate System (IS) Protocol is a dynamic routing protocol that has been included in GOSIP Version 2. It operates in the network to support CLNP. It operates over either point-to-point links or broadcast subnetworks (e.g., 8802/3, 4, and 5). Functionally ES-IS: (1) enables ISs to dynamically find ESs that are attached to the same subnetwork, (2) enables ESs to dynamically find ISs that are attached to the same subnetwork, (3) enables ESs to locate each other on a single subnetwork, (4) when two or more ISs are attached to the same subnetwork, enables ISs to redirect ESs to the IS representing the most efficient route to a given destination, and (5) allows ESs to automatically configure their OSI addresses.

7.3.9.2 Connection-Oriented Network Service

Use of the CONS can improve efficiency when operating over a single logical connection-oriented subnetwork (e.g., a single X.25 subnetwork, a set of X.25 networks interconnected by X.75 devices, or an ISDN). Use of this service can, under certain circumstances, avoid the overhead associated with the CLNP and may permit interoperability with end systems that do not implement CLNP. Version 2 of GOSIP specifies procedures for using CONS to achieve interoperability. The CONS is an optional, additional service in GOSIP Version 2; the CLNP must still be acquired for all GOSIP-compliant systems.

7.3.10 Subnetwork Technologies

Different subnetwork technologies provide for transfer of data packets between adjacent nodes of a network. This corresponds to the lower portion of the Network Layer (Layer 3), the Data Link Layer (Layer 2), and the Physical Layer (Layer 1) from figure 8. The nodes of a wide area network are separated by long distances, whereas local area networks are usually contained within a small geographic area. This difference is responsible for the different technology used in the two types of networks. In addition, local area networks have the following characteristics: (1) ownership by a single organization, and (2) high data rate (usually 4 megabits/second or greater). In many cases the operation of wide area networks must depend on existing transmission facilities, such as the telephone system. The protocols that support wide area transmission in GOSIP are the CCITT X.25 protocols; local area networks in GOSIP are 8802/3, 8802/4, and 8802/5. In addition, an ISDN can be used as a network technology for GOSIP end systems. The functionality required to transfer data packets between "adjacent" nodes of a subnetwork is provided by the Physical Layer (Layer 1) and the Data Link Layer (Layer 2).

The Physical Layer allows for the correct pin settings and signaling techniques of interfaces to lines so that bits of data may be transmitted from one machine to another machine. Issues here involve the nature of the physical medium, and insuring that proper synchronization is applied for the transfer. There are a large number of Physical Layer specifications, depending on the physical medium employed. GOSIP does not mandate any particular physical interface standard.

The Data Link Layer takes the raw transmission facility provided by the Physical Layer and transforms it into a link that appears substantially free of transmission errors to the network layer. It performs this function by taking bits and forming them into data frames; these data frames are then transmitted sequentially. The Data Link Layer provides error detection and, optionally, correction (involving two computers directly connected) across a line between nodes of a subnetwork.

The Data Link Layer checks the number and position of bits received, and performs various calculations to determine if there is an error, e.g., if a "1" bit is accidentally received as a "0". Synchronization of sender and receiver is important in this layer. The Data Link Layer emphasizes "box-to-box" communications; that is, management of bits between directly-connected computers.

The portion of the subnetwork technology that resides in the Network Layer is responsible for routing and relaying within the subnetwork, if necessary. For instance, in an X.25 subnetwork, the X.25 Packet Layer Protocol provides for the internal routing (i.e., from switch to switch) of X.25 packets from one X.25 subscriber to another. Alternatively, in "8802" subnetworks, the Network layer component is logically empty, since the method of transfer is broadcast and there is no explicit subnetwork routing performed.

7.3.10.1 CSMA/CD (8802/3)

A CSMA/CD network consists of a series of devices connected to a cable (bus). Any device on the cable may transmit to any other device on that cable, by placing the destination address on the cable, along with data. Essential steps in the CSMA/CD protocol are given below:

(1) Listen before transmitting, to ensure cable is idle.

(2) A device begins sending a message on the cable, while at the same time "listening" on the cable and comparing what is being heard to the message it is transmitting.

(3) If transmission of the message completes with no discrepancy between what the device sent and what it "heard," then there was no collision and the message was successfully transmitted.

(4) If a collision is detected, then all transmission stops. The device (and other devices, if any, that participated in the collision) must wait, and then try again at a future time using a special "back off" algorithm.

This scheme works well for low to moderate loads (0-40 percent), because a station may transmit with little chance of collision. For heavy loads (above 50 percent), a device waiting to transmit may be indefinitely delayed, because of the frequent number of collisions encountered. This scheme is similar (but not identical) to Ethernet products that are currently in Federal offices. What the 8802/3-based products offer is minimal delay and reasonable throughput, particularly at low to moderate traffic loads. Also, CSMA/CD is fairly simple and inexpensive to implement.

7.3.10.2 Token Bus (8802/4)

The token bus technology uses a bus or cable architecture, similar to the previous local-area network, but in this instance a station needs a logical token in order to be able to transmit data on the line. This token is passed from station to station in a logical sequence (independent of the physical ordering of stations on the cable). Once the station has the token, it can send data via the bus to another station for a certain amount of time; in other words, it "seizes" control of the bus for a predefined time interval. When that time

expires, the station must relinquish the token. 8802/4 buses are generally implemented using a broadband cable, although a baseband option is available.

7.3.10.3 Token Ring (8802/5)

A token ring network consists architecturally of a number of stations connected to one another via a circular cable or loop. A token travels around the ring; this token confers on a station the ability to send data. When a station wants to send, it looks for the free token; if it is available, it grabs the token, changes it to a "busy" token, and appends data to it. The data travels around the ring to the destination station(s). When the data has been received by the sending system, it is removed from the ring. After a station has finished transmitting the last bit of data, it must regenerate the free token.

For lightly loaded systems, a station merely has to wait for the token to come around to begin sending, so there is minimal delay. There is no contention involved in token ring access, unlike the situation for CSMA/CD access. The primary token ring disadvantages are the complexity of the token ring scheme and the need for proper regeneration of lost or damaged tokens for the ring.

Care should be taken before specifying a requirement for 802.5. The chip sets available today do not support enough group addresses to work effectively with OSI routing protocols [MISC 5]. A common practice to resolve this problem is to use a different set of functional (multicast) addresses that are acceptable to OSI routing protocols.

7.3.10.4 ISDN

An ISDN (Integrated Services Digital Network) offers the advantages of (1) cost control (e.g., controlling access to the network), (2) high capacity (up to 100 times the data rate of conventional networks), and (3) flexibility (due to its ability of simultaneously transmitting voice, data and video from a single instrument). An ISDN may be used independently of OSI or as a network technology supporting OSI applications. An ISDN can be the network technology directly serving the end system or function as an intermediate subnetwork.

GOSIP references two combinations of channels on the ISDN digital bit pipe: (1) basic rate, which provides a minimal level of capability, and (2) primary rate, which provides an expanded set of capabilities over the basic rate Interfaces refer to the boundaries between the customer's equipment and the carrier's equipment. GOSIP also addresses the S, T and U reference points (defined in section 6).

The NIST Workshop Agreements give procedures for accessing an ISDN so that end systems using these procedures can obtain ISDN services and can successfully interoperate. Additional procedures may be implemented as long as they do not create system interoperability problems.

Incompatibilities still exist between ISDN switches of different manufacturers and between ISDN switches and terminals. Terminal adapters may be used to minimize or solve these problems.

Section 2.7 of the NIST Workshop Agreements give information on two fundamental ISDN services for X.25 packet mode ISDN terminals, as follows: (1) the ISDN provides a circuit mode (Layer 1) connection either on demand ("switched") or permanently ("dedicated circuit"), and (2) the ISDN provides the X.25 virtual circuit service. Appropriate ANSI, CCITT and ISO documentation for ISDN is given in the References section and in Appendix B. More information on ISDN capabilities is given in Appendix A.

A trial was recently conducted with three objectives: (1) to determine whether ISDN capabilities should be included in GOSIP, (2) to determine whether ISDN could be used as a subnetwork technology supporting OSI applications, and (3) to demonstrate the interworking of ISDN and existing subnetwork technologies. Documentation on the trial is available [NIST 7].

Information on operation in asynchronous (start/stop) environments is given in CCITT Recommen-

dation V.120. Q.921 and Q.931 provide for Switched Virtual Circuit (SVC) support of GOSIP over time at many government locations. Dial-up requirements could also be supported by CCITT X.31 in some configurations. Guidance on operation of asynchronous dial-up communications environments, based on implementation agreements for ISDN terminal adapters, is also in V.120. Work on this subject is also underway in the ISDN NIU-Forum (see sec. 10).

7.3.10.5 Local Area Network Bridges

Local area network (LAN) bridges are devices that connect LANs of the same or different type. The bridging occurs at the Data Link Layer (Media Access Control–see Appendix A) and is therefore transparent to the systems attached to the LANs; the bridged LANs appear to operate as if they were a single subnetwork, with messages transmitted on one LAN being automatically transmitted on the other by the bridge.

A variation of the bridge, a learning bridge, serves an additional function, that of transparently isolating traffic. These bridges observe the source link level addresses of packets that are transmitted, and learn which addresses are on which LAN (s). Subsequently, packets that originate on one LAN with a destination address on the same LAN are not transmitted onto the other LAN (s). This allows LANs to be bridged while avoiding the extremes of LAN traffic congestion that might result.

Currently, bridges between 8802/3 local area networks are prevalent. The GOSIP FIPS does not explicitly reference LAN bridges, and so their use is not precluded as long as their use does not compromise GOSIP local area network functionality. Choosing between LAN bridges and GOSIP routers in specific applications is an engineering issue to be decided based on engineering considerations.

7.3.10.6 X.25 Wide Area Network Technology

For transmission over long distances, existing public network facilities are often used. Since there are so many types of devices that could be attached to such facilities, it is desirable to standardize protocols for network access. The X.25 protocols fill this need. X.25 defines an interface between a DTE (data terminal equipment) and DCE (data circuit-terminating equipment). The DCE is the network interface point (owned by the network), and the DTE corresponds to user terminals (owned by the user).

The X.25 protocol establishes a virtual circuit between two machines; this is a definite path connecting the two machines through intermediate machines. This path is valid for the lifetime of the connection. Source and destination addresses, as well as other information, are put on a call setup packet; data packets follow.

The X.25 packet layer (layer 3) protocol is concerned with data format and meaning in a frame, as well as subnetwork routing and virtual circuit management. When one system wants to connect to another system, a logical circuit is set up between them; there are a number of parameters which specify various kinds of information. Some functions are: reset, and clearing a circuit (when a call request cannot be completed). The restart command clears all virtual circuits between specified DTE and DCE.

The 1984-based X.25 protocols offer enhanced capabilities from the 1980 Recommendation to support OSI applications, such as Network Layer addressing and quality of service provision. GOSIP requires 1984 X.25 in Version 2.

To transit from a 1980-based X.25 system to a 1984-based X.25 system, the following advice is given: 1) if an agency uses 1980 X.25 in an end system or intermediate system and the SNDCP is not implemented as in IS 8878 Appendix A, then interoperability with 1984 X.25 systems depends on the internals of the network, and 2) if an agency uses 1980 X.25 in an end system or intermediate system and the SNDCP is implemented as in IS 8878 Appendix A, then interoperability with 1984 X.25 systems must be implemented in compatibility mode as in Appendix B of IS 8878.

7.4 Implementation Alternatives

7.4.1 General

It is important to understand that the OSI architecture gives vendors great flexibility in determining how the protocol standards are implemented. The interface that is specified between adjacent layers is an abstract definition that was created in order to describe the services that the lower layer offers to the upper layer. However, vendors are not bound to implement discrete processes corresponding to the functionality of each layer with accessible service interfaces between the layers. For example, a vendor may decide for reasons of efficiency to merge the functions of the Presentation and Session Layers in one process without an exposed interface between the layers. As long as the protocol information that is transmitted between the Presentation and Session Layers of the local system and the communicating end systems can be interpreted by both systems, the implementation conforms to the international standards for these protocols.

The way an interface will be implemented depends to a certain extent on the way the adjacent protocol layers are implemented, and to a great extent on the operating system environment. Basically, there are two categories: an open or accessible interface, and an embedded interface. An embedded interface is "invisible" to program users. The protocols are enmeshed and entangled so that there is no clear boundary between them. In an open interface, there appears to be a clear, well-defined boundary separating two distinct pieces of code. Figure 10 illustrates this. Issues may be raised pertaining to the characteristics of a (1) user interface, or (2) application interface.

Users may have reasons to request that the vendor provide an accessible interface to one or more layers in their implementations. An accessible Transport Layer interface allows a user to write software which uses the services of OSI layers 1-4 to reliably transfer data between different end systems. An accessible interface to the Association Control Service Element (ACSE) allows different applications to access the ACSE to perform common application layer services, as described in section 7.3.1. An accessible interface to the MHS Message Transfer Agent allows users to write their own User Agents which use the services of the Message Transfer System to transfer information to each other.

The OSI end system functionality need not, and frequently will not, be implemented on one stand-alone processor. For example, implementing OSI layers 1-4 on a front-end processor can free a central processor from the input/output overhead and allow it to perform other tasks more efficiently. The front end processor is also able to act as a concentrator servicing more than one mainframe. The user interface and the application layer functions for FTAM and MHS can be implemented on terminals or workstations which access a central processor for lower-layer services. Similarly, Transport Layer functionality may be implemented in a number of different ways. The benefits and tradeoffs for each implementation alternative will vary with the situation and they should be examined carefully while configuring an OSI system.

7.4.2 MHS Implementation Choices

The User Agent can be implemented in the same processor as the local Message Transfer Agent or in another processor at a remote location. The User Agent can be supplied by the same vendor that supplied the Message Transfer System or by a different vendor. The User Agent and Message Transfer Agent can be consolidated in one processor with access to the User Agent by desk-top personal computers provided by non-standard terminal emulator software. There are many options for configuring a Message Handling System and the advantages and disadvantages of these options will vary with each Federal agency. Procurement authorities should be aware of the options and, if nesessary, consult with vendors about available alternatives before issuing a solicitation document. Further guidance is available in NIST Evaluation Guidelines for Message Handling Systems [NIST 3].

All User Agents provide services which are not subject to standardization. User Agents assist the originator to create and edit a message and store the message until the recipient is ready to read it. Federal agencies that have specific requirements for nonstandard User Agent services should specify these requirements in solicitation documents.

The Message Transfer System and the Interpersonal User Agents (see Appendix A) provide the capability

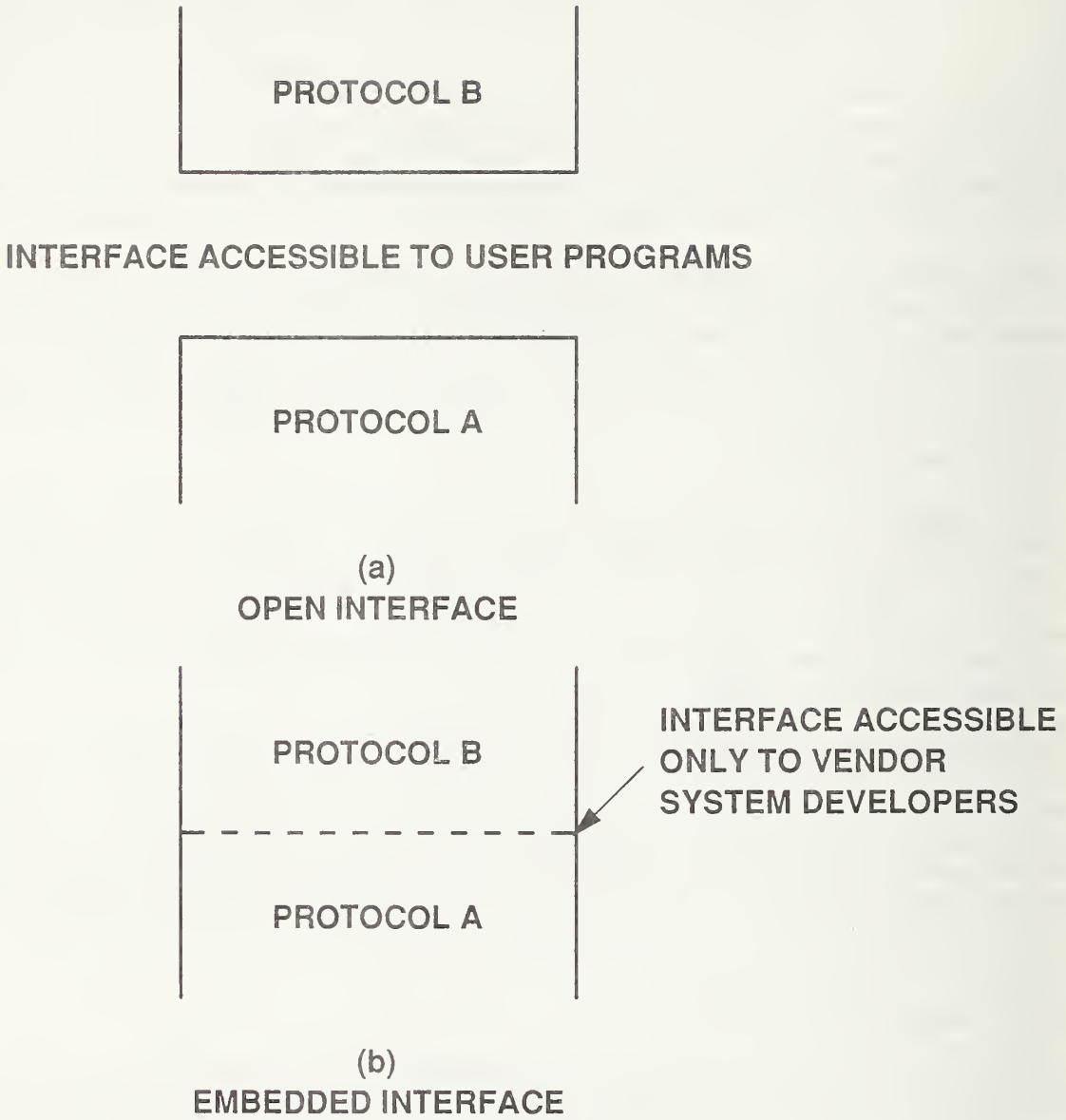


FIGURE 10
OSI SERVICE INTERFACE CHOICES

of transferring electronic mail between human users. Other special-purpose User Agents can be written which use the services of the Message Transfer System, if the vendor provides a means for these User Agents to interact with the Message Transfer System. Federal agencies that have a requirement to write or procure their own User Agents should specify in their solicitation documents that a programmable interface to the Message Transfer System is required.

Vendors who have previously marketed electronic mail systems may preserve their existing user interface when building MHS products. The system will be programmed to recognize when a recipient address is non-local. Special relay routines will then format the message in accordance with the CCITT MHS Recommendations. Preserving the existing user interface has the advantage of requiring a minimum of training for users of the old system; however, in this case, the ability for a user to generate certain optional Interpersonal Message service elements (e.g., Expiry Date, Cross-Reference Indication) may not be provided. Procurement authorities should be aware of these optional Interpersonal Message service elements (see Appendix A) and insure that services that are critical to their mission are specified in solicitation documents.

The MHS Recommendations describe body parts other than IA5 (ASCII) text. A GOSIP option allows users to specify that their Interpersonal User Agents be able to process body parts other than IA5 types. Other specifications (i.e., TOP Version 3.0 [MISC 2]) mandate this capability. This option is mandatory if GOSIP is to be used in a CALS environment (i.e., exchange of data formats such as IGES, CGM, SGML, etc.).

The NIST Workshop Agreements [NIST 1] allow limited flexibility in the Transport and Network Layer services used by MHS implementations. Procurement authorities should specify that Transport and Network Layer services they require when procuring a Message Handling system. For an expanded discussion see Appendix A.

Implementations of Session (and Transport) supporting MHS could be bundled or separate from each other and from MHS implementations. Session or Transport could be implemented on a front-end processor, communications processor, or on each host. Sender and receiver portions could be implemented together or separately. Figure 11 gives some implementation styles relating to the MHS protocol.

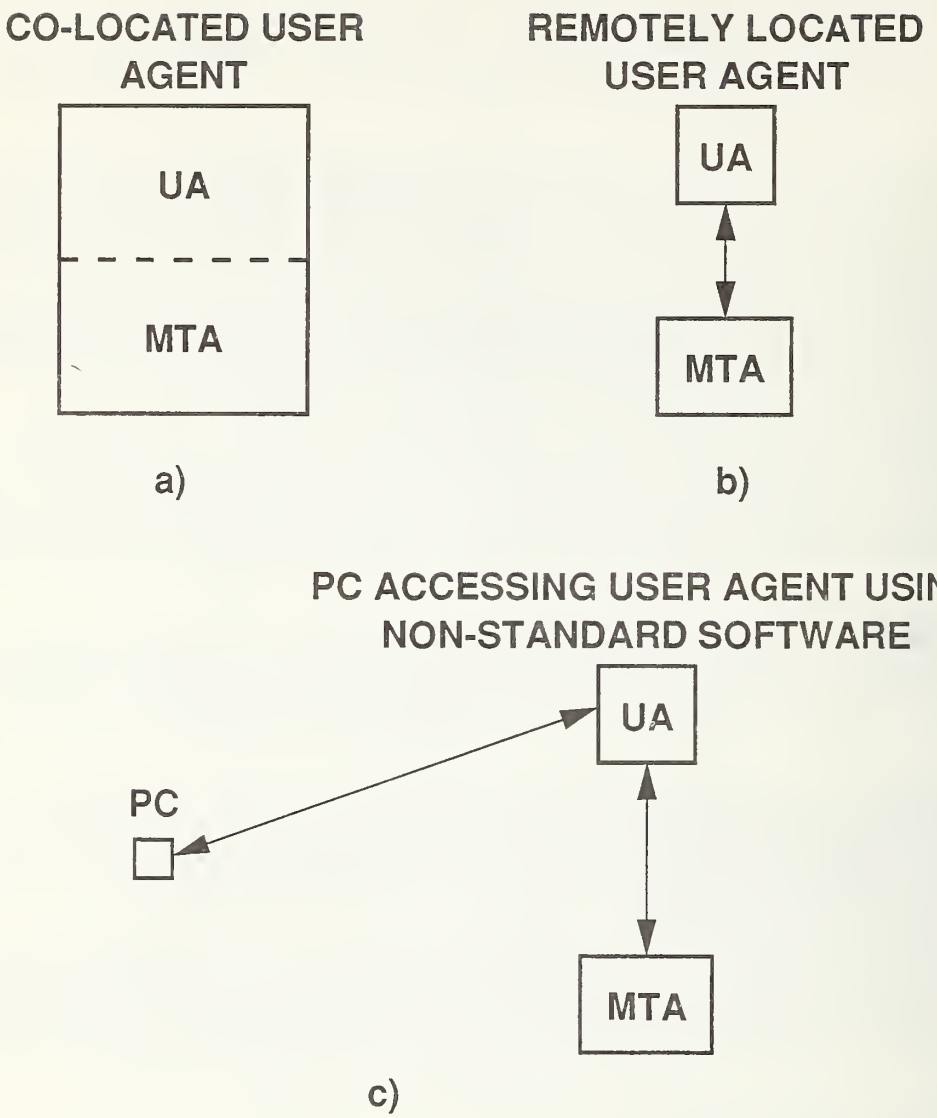
Version 1 of GOSIP originally required that private messaging systems within the government be capable of routing on administration name, private domain name, org name, org unit, and personal name. In an addendum to Version 1 of GOSIP, the requirement that private messaging systems be capable of routing on personal name was dropped. This change expands the range of messaging systems that are potentially GOSIP-compliant.

7.4.3 FTAM Implementation Choices

FTAM may be viewed as a series of callable library routines designed to serve other applications or processes. There is no standard FTAM user interface; a special user interface may be requested to accommodate individual requirements. FTAM may also be integrated into existing file transfer software and/or remote file systems.

FTAM may be implemented in terms of the initiator or responder (or both), and in terms of a sender or receiver (or both). FTAM may be implemented on a front-end processor, file server, communications processor, or on a host or workstation. FTAM functionality may be available directly or remotely; for example, FTAM does not have to be implemented on every PC, since these services may be made available in other ways. FTAM may be integrated directly in a local system environment (operating system), or separately.

It might be more cost effective to implement an FTAM product on a small number of servers, rather than on each individual host, particularly if the number of hosts is large and a convenient means exists of using FTAM via the server.. Proprietary software could then handle the conversion between an existing file protocol on each host and FTAM. This means that code on each host would not have to be changed to



PC = PERSONAL COMPUTER
UA = USER AGENT
MTA = MESSAGE TRANSFER AGENT

FIGURE 11
MHS IMPLEMENTATION CHOICES

accommodate the installation of the FTAM protocol on each host.

As a convenience to users, FTAM defines special functional profiles called Implementation Profiles. There are six Implementation Profiles defined: Simple File Transfer (T1), Positional File Transfer (T2), Full File Transfer (T3), Simple File Access (A1), Full File Access (A2), and Management (M1). One category in each class may be selected (e.g., T2, A1, and M1), or a category may be excluded (e.g., A1).

These Implementation Profiles are defined in terms of service classes, attributes, and document types. A user would evaluate conformance claims to one of these profiles based upon requirements stated in the NIST Workshop Agreements [NIST 1]. The simplest profile is T1; support of this is required of all FTAM systems. In general, higher-numbered profiles are supersets of lower-numbered profiles in the same class. For a maximum set of FTAM functionality, a user would require T3, A2, and M1.

Descriptions of what the profiles contain are given in the NIST Workshop Agreements. Each profile contains a set of functions which can be directly evaluated. For example, an inventory control system would include T2, A1, and M1, whereas a spooling application would require only T1 and M1. Each of the Implementation Profiles contains optional features as well.

FTAM may be "bundled" with any other modules, or exist as a separate module. In certain cases, FTAM cay be completely integrated with an existing file system, either local or remote. Implementations may use either an "external" or "internal" file service.

For a multi-user computer system, one might implement the kernel, storage, and security virtual filestore subsets. For a centralized database system, one would also implement the kernel, storage, and security subsets.

Some engineering issues for the user to consider are: extensibility, timer values, data item size, and efficiency, as well as synchronization. Other issues to consider are filesize, file naming, concurrency control, security, access control, audit capability, encryption, and error recovery.

NBS-9 is an optional document type in the NIST Workshop agreements. NBS-9 is important for file directory capability. NBS-9, for each file in the filestore, depicts a set of "read-attribute" values. These values, for storage, security, kernel and private use attributes, specify desired attributes for each file. Other document types are also important. Some of these are NBS-6 (sequential), NBS-7 (random access), and NBS-8 (indexed sequential).

The FTAM initiator and FTAM responder may be implemented together or separately depending upon particular agency configurations. Implementation profiles have been defined to enable users to implement FTAM more efficiently. Server implementations are defined in terms of file servers and print servers, among others. File servers may be implemented on a variety of different devices, and require only responder functionality in most instances. Print servers offer a more limited set of capabilities, and could be implemented on various special-purpose devices. For more FTAM information, consult Appendix A.

Presentation and ACSE code may be implemented together with FTAM (or with each other) or separately. Presentation or ACSE may be implemented on a host, front end processor, or communications processor. Functionality may be available directly or remotely. Sender and receiver code may be implemented together or separately. Transport and/or Session code supporting FTAM may be implemented together with FTAM or separately as well. Figure 12 gives some implementation choices relating to FTAM.

7.4.4 VT Implementation Choices

Before data can be transferred between the terminal and the remote host, the services and the virtual terminal environment must be negotiated and agreed. The services include communication mode, class subset and type of delivery control. The communication mode can be synchronous or asynchronous. The class subset refers to the level of negotiation of the virtual terminal environment that is permissible during

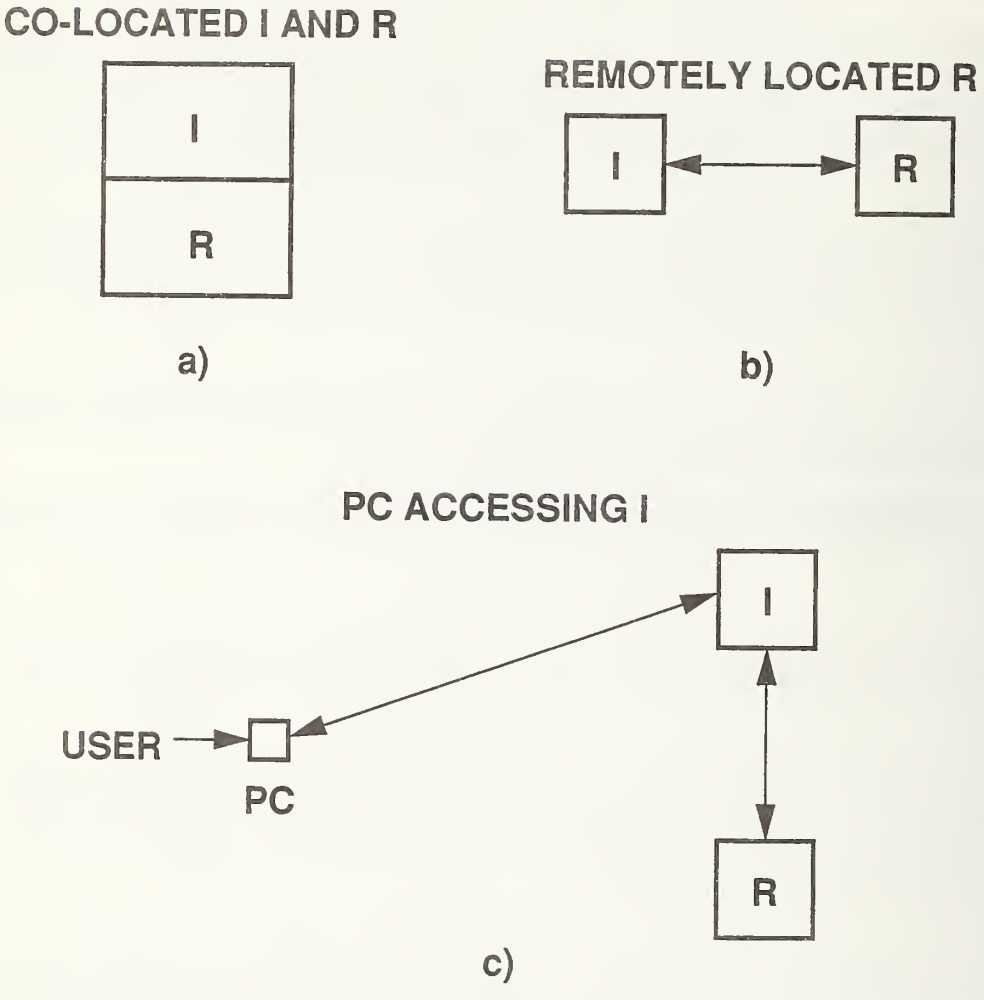


FIGURE 12
FTAM IMPLEMENTATION CHOICES

an association. Delivery control refers to when VT data is made available to the user at the remote VT implementation. These services are more fully discussed in the VT tutorial in Appendix A.

The virtual terminal environment conceptual objects that must be negotiated are display objects, control objects and device objects. A predefined set of these objects is called a profile.

A display object is a mechanism through which a terminal's display screen and keyboard are modeled. Profiles with one display object are called S-mode profiles and are intended to model the operation of a synchronous terminal. Profiles with two display objects are called A-mode profiles and are intended to model a traditional asynchronous terminal. Some primary parameters are: display-object-name, object-access-right, dimensions, erasure-capability, and repretoire-capability. Some secondary parameters are: X-bound, X-addressing, X-window, and font-capability.

Some control object parameters are: CO-name, CO-type-identifier, and CO-priority. Device objects are used to model characteristics of real devices and are intended to assist in mapping display objects to those real devices. Some parameters are: device-name, device-display-object, and device-default-CO-access.

The Telnet profile supports a simple line at a time or character at a time dialogue. The forms profile is intended for terminals with microprocessors that are capable of validating the data entered at the terminal before it is transmitted to the remote host. The Transparent profile supports the exchange of uninterpreted sequences of characters. This includes VT users who wish to control terminals directly through the use of embedded control characters and escape sequences. ISO has specified default profiles for each terminal type.

There is no standard for a VT application program interface. The VT protocol may be integrated into the terminal I/O subsystem of the operating system and so remain invisible to applications. Any of the VT profiles could be used directly by applications in a variety of ways which would require a programmable interface. Federal agencies that have a requirement to develop applications that use VT services directly should specify that as a requirement in their solicitation documents.

There are no standards for a VT user interface, although a user community may prefer a particular user interface. Federal agencies requiring specific user interfaces should specify those interfaces in their solicitation documents.

VT implementations may support initiator or responder roles or both. VT may be implemented in front-end processors for hosts or workstations that do not yet have native VT implementations, or may be implemented directly on the host or workstation.

VT can be used to create a distributed environment at the level of terminal- to-host access so that any terminal can be associated with any host. With the Forms-1989 VT profile, a system could support an application that could act as a centralized Forms Server, and so support multiple client systems from a central system acting as repository of forms applications and forms data.

There are several points in the protocol stack where a machine boundary could be inserted, but, unlike FTAM or MHS, the performance of VT is dramatically visible to the user, so it is better to split the processing at a simple interface such as Transport or Session, rather than at higher points in the protocol stack. Tutorial information on VT is given in Appendix A.

7.4.5 Performance

Each agency must determine specific performance requirements, if any, for inclusion into RFPs citing GOSIP. For each protocol considered (e.g., X.400, FTAM, end-to-end transport) different performance criteria may be of interest. Performance measures of general interest usually include delay, throughput, capacity, response time, availability, and reliability. Of course, to be measurable such performance parameters must be precisely defined.

The NIST is working to develop performance and functional evaluation guidelines for GOSIP. Documentation [NIST 3] is available for the MHS application, and is under development for the FTAM application. Previous work completed by the NIST is available now, but focuses only on end-to-end transport performance. Until the NIST guidelines are complete, agencies may desire to work directly with the NIST on specific procurements.

Two possible levels of performance to consider are: end-to-end (Transport Layer) performance, and application-level performance. Some factors which may affect performance at the Transport level are: network diameter, window size, network load, packet size, and error rate. In terms of management, some factors to consider are: reliability, redundancy, response time, and ease of configuration.

Currently performance is not standardized under the scope of the OSI Reference Model. Agencies should develop performance criteria based upon internal needs. Important performance metrics and benchmarks for a particular agency should be defined. Then, with vendor consultation, the agency should determine what is practical and achievable, given current architectural and technology constraints.

Application-level performance requirements should include measurements of user-to-user throughput and acceptable end-user delay time under a set of typical loads. An end-system user may also be interested in a measure of reliability or robustness for a particular application. A typical performance metric to consider is the capacity of a system (e.g., the number of simultaneous connections). When performance data is available, this information may assist in precisely defining performance requirements in solicitations.

7.5 Technical Information in Product Announcements

Technical information in vendor product announcements will stress the OSI-based services provided. Both OSI terminology and vendor-specific terminology are likely to be employed. Upon receiving a product announcement (or a response to a solicitation), the technical specialist should examine and interpret it in the following manner: (1) make a list of essential agency OSI functional requirements, (2) make a list of OSI services provided by the vendor, (3) match the two above-defined lists to determine whether all of the agency's functional requirements are satisfied, and (4) consult this Guide (and other appropriate documents) to understand the technical material in the announcement. It is possible, upon performing this list comparison, that product features will emerge that were not on the "agency requirements" list; if this is true, then these could be added to agency requirements.

Agency officials should ensure that vendor enhancements to the GOSIP FIPS (1) do not compromise basic OSI functionality, and (2) do not adversely affect GOSIP interoperability. Subject to these constraints, users may request and encourage enhancements to GOSIP-compliant products from vendors.

7.6 GOSIP Application Information Flow

This section references the Application Layer protocols (FTAM, MHS, VT) contained in the GOSIP FIPS. The intent is to give an elementary understanding of the workings of the Application Layer protocols.

7.6.1 FTAM Example

The steps to accomplish an FTAM activity are listed below.

(1) A user issues an FTAM initialize service primitive, with the appropriate parameters included.

(2) After success, an FTAM select is issued if a pre-existing file is to be selected; otherwise an FTAM create is issued if a new file is to be created.

(3) After success, an FTAM read attribute is issued to interrogate the properties of the file; an FTAM change attribute may be issued to change the properties of the file.

(4) An FTAM open may be issued to gain access to the contents of the file. The context and format of

the file is negotiated at this time.

(5) An FTAM read or FTAM write is issued, depending on whether the file is to be read or written. FTAM data commands transfer data. FTAM "data ends" terminate the data flow in one direction, and FTAM "transfer ends" terminate the total data transfer. FTAM cancel interrupts an existing data transfer.

(6) An FTAM close releases access to the contents of a file.

(7) An FTAM "deselect" releases access to the file's properties; an FTAM delete eliminates the file.

(8) An FTAM terminate ends the file activity normally. An FTAM abort abruptly ends the file activity (because of an error).

7.6.2 Message Handling Systems (MHS) Example

In a Message Handling System, or X.400 implementation, the steps taken by a process wishing to send mail to a recipient process are listed below.

(1) The originator specifies the message to be sent, to whom it should be sent, and which Message Transfer services are being requested (e.g., priority delivery or delivery notification).

(2) The user agent submits the message to the local MTA. The MTA accepts responsibility for delivering the message to all recipients.

(3) The MTA acts like a post office and relays the message to other MTAs depending on the destination address. This message may cross different management domains.

(4) A message consists of an envelope and contents. The information that the Message Transfer System normally needs to perform its task is on the message envelope. The Message Handling System does not examine the contents, except in rare instances, to convert the encoding of the message.

(5) When the message gets to the destination MTA, that MTA will recognize the address and deliver it to a local user agent.

(6) The user agent will attempt to deliver the message to a recipient, or store the message for later delivery.

(7) If there is a problem with delivering the message to the user agent, a nondelivery notification will be returned.

7.6.3 VT Example

Before VT data transfer can begin, the Virtual Terminal Environment must be established. The Virtual Terminal Environment defines the capabilities and contraints of the terminal and the services available during the VT association. A predefined set of parameters identifying the terminal capabilities and constraints is called a profile. The services which must be agreed prior to the initiation of data transfer include: class subset, which defines the extent to which parameter negotiation is permitted, the type of delivery control, and the mode of transmission. See Appendix A for a description of these services.

The Virtual Terminal protocol allows the exchange of data between Virtual Terminal Protocol Machines (VTPMs). One VTPM resides on the computer system serving the terminal; the other VTPM resides on the remote host. In the synchronous mode of transmission, there is a single abstract structure identifying the screen image on each VTPM that can be updated by both the terminal keyboard and the remote host.

When a user types on the terminal keyboard, a data structure is modified to reflect the changes, and those modifications are sent to the VTPM on the computer system serving the terminal. The updates are

then sent to the VTPM serving the remote host. The updates are used to create an identical copy of the data structure, and are made available to the application program. The same process occurs in reverse when the application program initiates the terminal update.

Since the two VTPMs maintain identical copies of the data structure, a token is used to control access. Only the token holder can modify the data structure and the token can be passed back and forth between the two VTPMs.

In the asynchronous mode, each VTPM has a data structure for input and a separate data structure for output. When a terminal user types on the terminal keyboard, the terminal input data structure is modified and the updates are transmitted to the output data structure on the remote host using the VT protocol, and from there to the application program. If, at the same time, the terminal output data structure is updated by data sent from the application program, the data is displayed at the terminal, perhaps overwriting data recently entered at the terminal keyboard.

In both modes, the VT protocol provides the ability to specify whether characters entered at the data terminal should be immediately echoed back to the screen, or whether the screen update should occur only as a result of actions initiated by the remote application process. Information about the terminal capabilities and constraints must be exchanged and agreed. This is normally done using a predefined set of parameters called a profile.

7.7 Future GOSIP Protocols and Services

Given below are descriptions of protocols under development and for incorporation into future versions of GOSIP. The appendices of the GOSIP FIPS give additional detail and scheduling information. Users should consider this information when making long-term procurement plans.

7.7.1 Transaction Processing (TP)

Transaction processing is an Application Layer protocol which is used for exchange of information between two or more distributed systems according to the ACID rules. ACID, as applied to a transaction, ensures: (1) atomicity (the total work is performed or nothing is done), (2) consistency (work is performed accurately and correctly), (3) isolation (while the work is being performed inconsistent data is not available to other transactions), and (4) durability (the work is fault-tolerant). This last point is especially important in the context of data base management. It means that enough information will be retained so that in the event of a system failure the information on the data base will be unaffected. A situation where transaction processing might be applied is given below.

An individual desires to fly to a specific city on a specific airline at a set time; that individual may also want to rent a certain car, stay at a certain hotel, apply for an advance, and see some clients. Without TP the traveller would have to make a separate reservation with the airline, with the car rental company, and with the hotel, as well as with the bank and clients. Each of these is a separate action; if there are problems with any one action, a drastic change in plans may be necessary. With TP, that individual would be able to first find out whether all of the actions could be completed successfully, and if they could, then that individual could direct that they be carried out as a single action. Other potential uses for TP are in banking transactions, supply and accounting systems, and network management.

7.7.2 Secure Data Network System (SDNS)

The Secure Data Network System (SDNS) incorporates a set of security protocols and procedures that provide a number of security services in the OSI Reference Model (IS 7498/1) [ISO 1]. The SDNS is an example of implementing security in accordance with the OSI Security Architecture [ISO 19] that has recently been approved as an International Standard. The Security Architecture defines a number of security services that can be implemented at one or more layers of the OSI architecture.

The security services that are defined in the OSI Security Architecture and provided in the SDNS are: authentication, access control, confidentiality, integrity, and nonrepudiation. Protocols and procedures for providing specific security services at Layers 3, 4, and 7 are being developed for the SDNS. Specific algorithms for confidentiality, integrity, authentication, and key distribution have been specified.

The SDNS can be used in a variety of networks including local area networks, wide area networks and point-to-point communications networks. The SDNS offers comprehensive security in a number of network applications including electronic message handling and file transfers. The SDNS is intended to serve as the basis for protecting classified data as well as unclassified, but sensitive, data in a wide range of applications.

An updated optional security section is included in GOSIP Version 2. This provides for limited security capability at the Network Layer. This is still just a placeholder for future security services, but may be referenced if it meets user needs.

7.7.3 Network Management

As the number of networks and related services grows throughout the U.S. Government during the 1990s, requirements for integrated network management capabilities will become more urgent. Specifically, network operators will need to configure network resources, detect and correct faults, account for network use, monitor and adjust performance, manage security mechanisms, and secure network management information. Network components projected to be employed include GOSIP end systems and intermediate systems, ISDN switches, X 75 gateways, PBXs, modems, multiplexers, packet switches, leased point-to-point circuits, and local area networks.

The NIST is working for an environment where network components made by a variety of vendors can be managed from an integrated network manager without the need for proprietary management protocols. This will require (1) defining a set of interoperable protocols for exchanging management information, (2) agreeing on the structure of managed objects, and (3) defining the managed objects and related attributes. The NIST has issued a draft initial network management FIPS, called the Government Network Management Profile (GNMP). The initial GNMP concentrates on configuration and fault management at Layers 1-2 of the OSI Reference Model. The managed objects, attributes, and structure in the GNMP will be worked out with industry and user participation in standards meetings and other open forums. Additional versions of the GNMP will be issued as appropriate, based on completed international standards. The scope of the GNMP will expand over time to become a specification for integrated system and network management, including remote operating system and application management.

7.7.4 Fiber Distributed Data Interface (FDDI)

Fiber Distributed Data Interface (FDDI) specifications describe a token passing technology allowing for very high data rates over fiber optic links connecting systems. Instead of the 5-16 Mbit/sec data rates over typical local networks, data rates of up to 200 Mbit/sec are achievable using FDDI. Applications for this technology can include weather information processing systems, oil refinery drilling operations, and the space shuttle support program. End systems and software must be designed to effectively handle high-bandwidth FDDI transmission. FDDI systems can be useful as a campus network to connect local-area and wide-area network facilities in Federal environments.

7.7.5 IS-IS Routing Protocols

Dynamic routing allows the selection of an efficient route to a destination, based on such factors as congestion, path availability, and line charges. The protocols to perform this function between intermediate systems are the intermediate system to intermediate system (IS-IS) routing protocols.

IS-IS protocols provide for the dynamic routing of information between different subnetworks that are under the control of the same or different administrative domains. Work on standardizing these protocols for both the intra-domain case and the inter-domain case is progressing.

GOSIP-supported routing structures and domain specific (DSP) address formats are in alignment with the OSI IS-IS intra-domain routing protocol currently under development. Future versions of GOSIP will mandate the use of standardized OSI IS-IS routing protocols.

7.7.6 FTAM Extensions

In the future, the FTAM standard will be augmented to allow: (1) simultaneous reads and writes to a file (for use in database applications), (2) file directory manipulating capability (ability to search (list) directories), and (3) specification of different levels of access control on portions of files. These extensions will increase the flexibility of applications that use FTAM.

7.7.7 X.400 (MHS) Extensions

The Message Handling Systems (MHS) specifications in Version 2 of GOSIP are based on the 1984 CCITT Recommendations. The GOSIP MHS extensions will be based on the CCITT 1988 Recommendations. Services that will be considered for future versions of GOSIP include security, message store delivery, use of directory services (see sec. 7.7.8), a User Agent for Electronic Data Interchange, and an OSI architecture which includes ACSE and the Presentation Layer.

The security features include message originator authentication, checks against unauthorized disclosure and verification of content integrity. Message store delivery allows personal computers without full User Agent functionality to access MHS services.

MHS implementations conforming to the 1984 Recommendations sit directly above and use the services of the Session Layer. Implementations conforming to the OSI architecture specified in the 1988 Recommendations will be backwardly compatible with the earlier implementations.

7.7.8 Directory Services

The ISO/IEC has issued the Directory standard as ISO (International Standards Organization) 9594; the CCITT has released Recommendation X.500, which is technically aligned with ISO 9594. The Directory standard provides a facility for storing and retrieving information about objects in the OSI environment. For each object the Directory maintains an association between the object's name and its attributes. Examples of standardized attributes for processes include OSI service access point addresses and electronic mail originator/recipient names. Typical attributes for a Directory entry on an individual include electronic mail name, telex number, telephone number, facsimile address, and postal address.

Using the Directory to provide addressing information about an object based on the object's name can shield OSI users from underlying changes in the network. A limited browsing facility is supported to aid users in identifying names. The Directory also supports a "yellow pages" service, capable of providing users with names of all objects having specified attributes (e.g., all devices connected to address 0123).

Requirements for initial GOSIP directories include: 1) name to data record mapping, 2) host name to network address mapping, 3) service name to selector mapping, and 4) resolution of mailing list names into electronic mail addresses. In addition, access control, simple authentication and replication will be required. The Federal government is planning to develop a nationwide Electronic- Directory Pilot, based on the standard, to further government directory services user needs.

7.7.9 Future Virtual Terminal Profiles

The Basic Class VT Protocol allows terminals and hosts on different networks to communicate without requiring that one side know the terminal characteristics of the other side. A generic set of terminal characteristics is defined for communication which is mapped to local terminal characteristics for display. An addendum to Basic Class VT provides a forms mode capability.

A set of parameters developed to describe a particular type of terminal is called a profile. Future versions of GOSIP may include the X.3, scroll, forms and page profiles.

7.7.10 Transport Class 2

The Transport Protocol Class 2, for use over the connection-oriented network service (CONS), is accepted by several OSI profiles. The Class 2 Transport Protocol is used with CONS in several Federal government applications, where communication is confined to a single logical subnetwork.

The specifcation of the Class 2 Transport Protocol as an option in a future version of GOSIP would be intended to enable interoperability among Federal government computer systems when using Class 2 Transport over CONS. The ability to choose the correct transport protocol class for a given instance of comunication will require a priori knowledge on the part of the transport connection initiator, until directory services are included in GOSIP. TRANSPORT CLASS 4 IS REQUIRED AND WILL CONTINUE TO BE REQUIRED FOR ALL GOSIP SYSTEMS.

7.7.11 Electronic Data Interchange (EDI)

Electronic Data Interchange (EDI) describes the rules and procedures that allow computers to send and receive business information in electronic form. This includes the full range of information associated with buyer/seller relationships (e.g., invoices, customs declarations, shipping notices, purchase orders). The CCITT has standardized a User Agent that will use the services of the Message Transfer System (as specified in the CCITT 1988 MHS Recommendations) to transfer this business information. The use of MHS to convey EDI information is a GOSIP advanced requirement.

7.7.12 Remote Data Base Access

Remote Data Base Access (RDA) allows the interconnection of database applications among heterogeneous environments by providing standard OSI application layer protocols to establish a remote connection between a database client and a database server. The client is acting on behalf of an application program while the server is interfacing to a process that controls data transfers to and from a database. RDA is a GOSIP advanced requirement.

7.7.13 Manufacturing Message Specification (MMS)

The Manufacturing Message Specification (MMS) application can be used to obtain and/or manipulate objects related to a manufacturing environment. These objects include, but are not limited to, variables, semaphores, data types, and journals. Although MMS was designed for a manufacturing environment. these objects have applicability outside of manufacturing. MMS is currently a GOSIP advanced requirement.

8.0 REGISTRATION

8.1 Motivation for Registration

In order to communicate, it is necessary to identify the objects involved in communication. These objects have names and addresses. A name is a collection of attributes that identify an object within a domain. An address is a name that is used to specify the location of an object. The names must be registered with a registration authority so that they will not be used for more than one object (i.e., names must be unambiguous).

Without registration authorities, chaos will result, because random name and address values will be assigned to objects. Since systems would not be able to uniquely identify themselves globally, communication would become impossible. Verifying the existence of connections would become impossible; routing of protocol information would become cumbersome. For all of these reasons, registration procedures are essential in the OSI environment.

If an organization does not ever intend to communicate with "outside" organizations (where "outside" is agency-specific), then an organization need not be bound by any addressing recommendations contained herein. However, if an organization intends to communicate with "outside" organizations, then the recommendations in this section comprise a viable consistent mechanism for assigning values.

General OSI addressing and registration are described in section 8.2. Objects which need to be registered for the Government Open Systems Interconnection Profile (GOSIP) Federal Information Processing Standard (FIPS) are described in sections 8.3, 8.4, and 8.5. For planning purposes, objects which will need to be registered in future GOSIP versions are mentioned in section 8.5.4.

Detailed registration procedures for users are given in a GOSIP Registration Services Document [MISC 6] published by the U.S. General Services Administration (GSA). Finally, a summary for users is given in section 8.7.

GOSIP Version 1 implementations should use the Network Service Access Point address format described in section 8.3; this format is aligned with routing standards being developed by the ISO/IEC.

8.2 Theory of OSI Address Assignment

OSI names and addresses consist of attribute-value pairs which are hierarchical in nature and which combine to uniquely identify or locate an OSI object. Since the relationship between the components of a name or address is hierarchical, it follows that the registration authority for names and addresses should also be hierarchical. A governing organization does not always have sufficient knowledge of organizations lower in the hierarchy to wisely assign values within those organizations. Thus, an approach frequently taken is to delegate registration authority to the lower organizations in the name or address hierarchy.

Hierarchy implies a "treelike" structure where the number of objects increases from the "top" of the tree to the "base" of the tree. The tree may be sliced into horizontal "levels"; level one corresponds to the "top" of the tree, and the highest-numbered level corresponds to the "bottom" of the tree (or base). At the top of the tree, there is one designator that is most "powerful"; that is, it has the greatest scope of authority (largest domain). This designator assigns identifier values to objects under its authority. These objects have smaller domains than the objects immediately above. Each of these objects has a smaller scope of authority than the objects immediately above. This process goes on continuously, moving down the tree. Figure 13 illustrates this concept.

Important concepts are that the scope of authority decreases as one moves down the tree, and that the number of objects increases as one moves down the tree. One authority at a specific level may create zero, one, or many subauthorities at the next higher level. The number of levels in such a treelike structure is arbitrary.

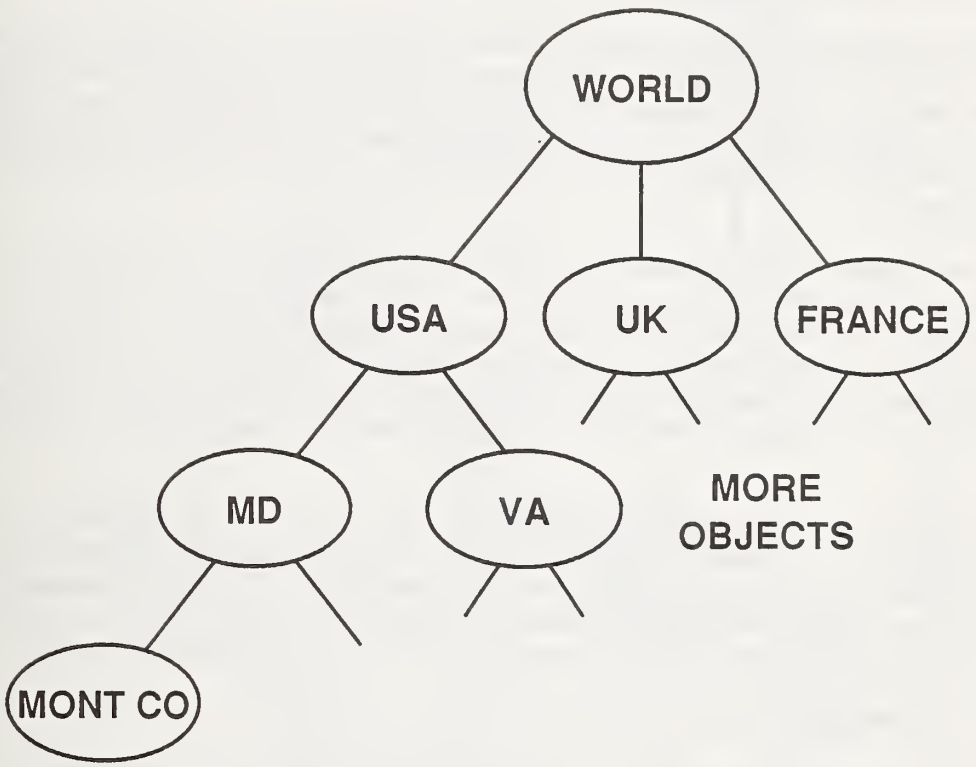


FIGURE 13
HIERARCHICAL TREE STRUCTURE

Taking a path through the tree from "top" to "bottom," and collecting all the identities moving from top to bottom, one constructs a sequence of attributes which may be read to get a unique specification for an object. For example, a path in figure 14 for Agency A under the International Code Designator (ICD) may be read as the sequence of identifiers iso, identified organization, ICD [5], Agency A [x].

No one element in the sequence is necessarily unique, but all the elements considered together in the proper order are unique as a group. Also, each element with the same immediate parent is unique at its level. The term "sequence" implies a definite ordering of elements. To create a unique sequence, an ADP system may "pick off" elements in a path down the tree, and append each selected element to the end of the list of previously-selected elements. To decode or "parse" a unique sequence, an ADP system will read the elements of the sequence in the order encountered from the beginning of the sequence, and construct a "path" in the hierarchical identification tree.

Registration authorities are created to register names of objects and, in some cases, to advertise these names. For example, the telephone companies assign numbers to subscribers and publish some of the numbers in a telephone directory. In the OSI world, some names are included and registered in the standard. For example, in X.420 Message Handling Systems, International Alphabet 5 (IA5) Text has been assigned a body part identifier of 0. This identifier distinguishes IA5 text from other body parts that can be transferred by the MHS application.

If applications want to exchange objects not included in the standard, such objects must be registered somewhere, so that no one else will use the same number for a different body part or a different number for the same body part In the future, when a standard is approved which will require further registration of names, the procedure for registration and the registration authority will be approved at the same time. For standards which have been approved in the past, different approaches have been taken. While there are a number of possibilities for assigning identifiers, several approaches particularly relevant for GOSIP will be described.

Under ISO, there are two major naming hierarchies or "trees." One is under ISO 3166, Codes for the Representation of Names of Countries. Under that hierarchy, the United States has been assigned an alpha-2 code of US, an alpha-3 code of USA, and a numeric code of 840. Under US, American National Standards Institute (ANSI) has assigned the Federal Government the alpha code of "GOV" and the numeric code of "101." The U.S Government could be unambiguously identified in an international directory as:

iso(1) member body (2) US (840) GOV (101)

The NIST is responsible for assigning codes under code 101, and has delegated that authority to the GSA.

Another tree that falls under ISO is ISO 6523, Structure for the Identification of Organizations. The British Standards Institute has been delegated the authority by ISO to issue International Code Designators (ICDs). NIST has received ICDs of 0004, 0005, and 0014 and is authorized to issue organization names under those codes The three codes are used for the Open Systems Interconnection Network (OSINET), U.S. Government organizations, and the NIST/OSI Workshop, respectively. ICD 0004 has been delegated to OSINET. NIST has delegated the authority to assign Administrative Authority Identifiers (AAIs) in GOSIP NSAPs under 0005 to GSA. Another ICD, 0006, was issued to the Defense Communications Agency (DCA) acting on behalf of the Department of Defense.

8.3 Network Service Access Point (NSAP)

8.3.1 Background and Importance

In the OSI Reference Model, reliable data communications occur between two end systems, usually via one or more intermediate systems. End systems are terminus systems, where data transfers originate or terminate. Intermediate systems are "transit systems," through which information passes from one end

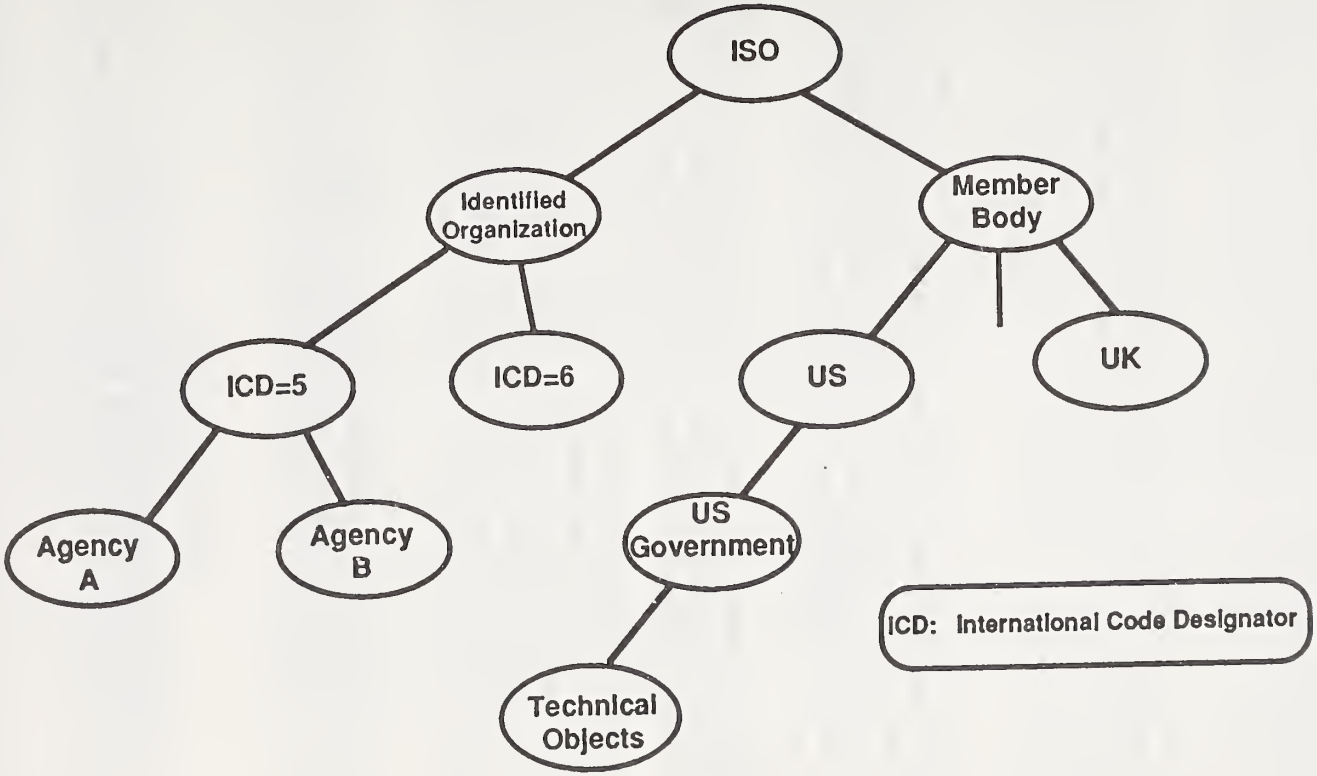


Figure 14
Sample Registration Structure

system (source) to the other end system (destination).

The terms "end system" and "intermediate system" refer to roles in transmittal of data and not to any special configurations. A system may be an end system or an intermediate system at different times or with respect to different data streams; such systems may be attached to local area networks or attached to wide area networks. Intermediate systems are used to interconnect subnetworks in OSI communications. An end system is usually controlled by a single authority. Any of the configurations shown in figure 15 may qualify as an end system.

Intermediate systems are used to link together subnetworks to provide paths connecting end systems. An end system may be connected to more than one subnetwork; similarly, a subnetwork may have multiple end systems connected to it. Figure 16(a) illustrates this in a hypothetical Federal environment; figure 16(b) shows the linking of subnetworks in a chain to connect two end systems. The actual physical connections are labeled as subnetwork points of attachment (SNPAs).

An NSAP is an identifier that uniquely distinguishes one end system from another in a network of systems. An intermediate system will "read" the NSAP address and determine where to send the packet (a similar function to that of a post office in reading an address for an envelope). Each NSAP is unique globally in the context of OSI; an NSAP value must be known to all other systems communicating with this system. The NSAPs themselves only have meaning to the communicating entities, such as OSI Network Layer service entities.

The NSAP also identifies a point at which network service is provided to the Transport Layer, which is responsible for the end-to-end transfer of data in the OSI model. There may be any number of NSAPs for an end system. These NSAP values must be known to the "end-to-end" communications software which runs in end systems. NSAPs are encoded as unique strings of characters (or numbers) that may be interpreted reading from left to right using the hierarchical model described previously. Each NSAP value in an end system specifies a different user of the Network Layer service.

From figure 16, intermediate systems route information based upon selected components of NSAPs received in transit. If the NSAP "matches" the system address, that system is in fact the destination system. If not, then a routing table is used to find the next system along the route to the destination.

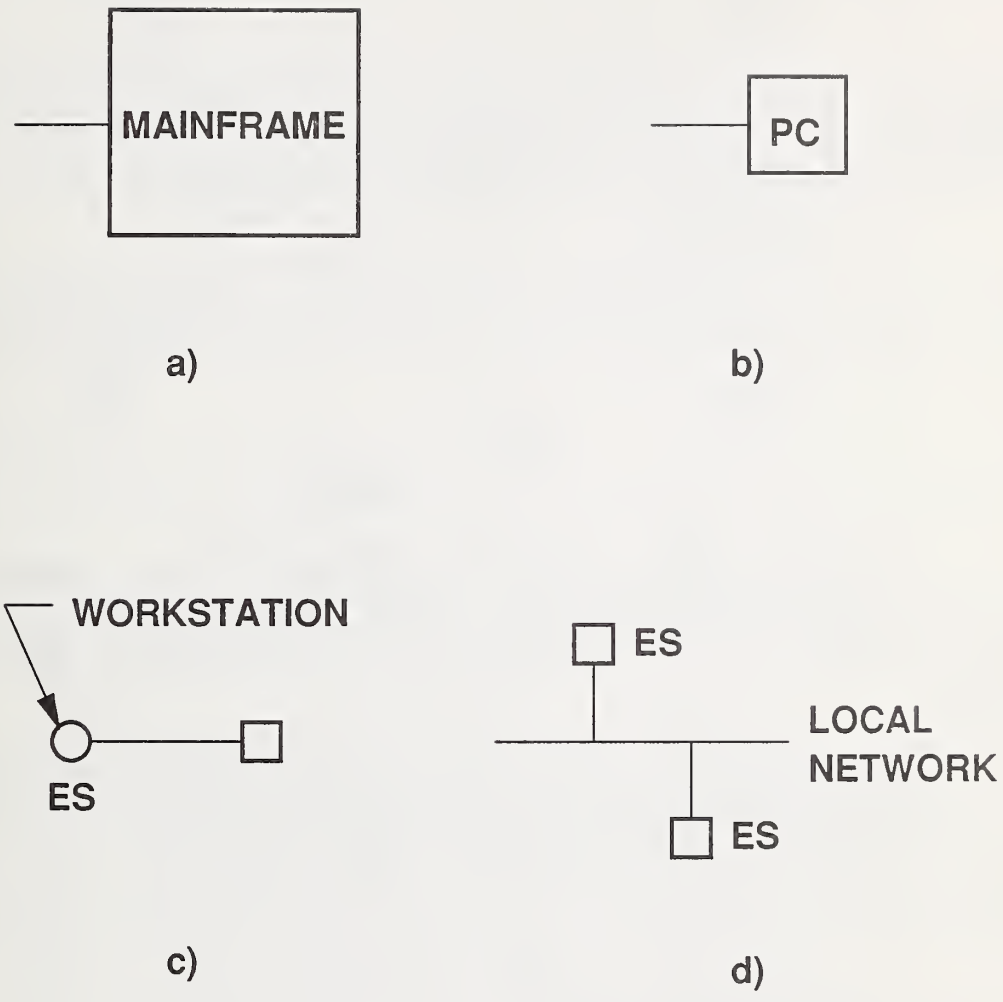
The NSAP is the only address in OSI that identifies end systems uniquely; all other OSI addresses identify intermediate systems or end-system processes. Globally unique NSAP addresses are important in the federal environment because increased communication across different subnetworks in a distributed global environment is anticipated. If every end system in all Federal agencies is assigned a unique address, then every end system, from PC to mainframe, can potentially communicate with every other end system. NSAPs are the first category of objects which must have registration authorities established to assure assignment of unique addresses for all.

In sum, an OSI network is composed of end systems on different subnetworks interconnected by intermediate systems. NSAPs identify the end points of network communications, or the service access points of the Network Layer. The NSAP selector (see sec. 8.3.2) allows different users of the Network Layer service to be distinguished.

8.3.2 NSAP Format

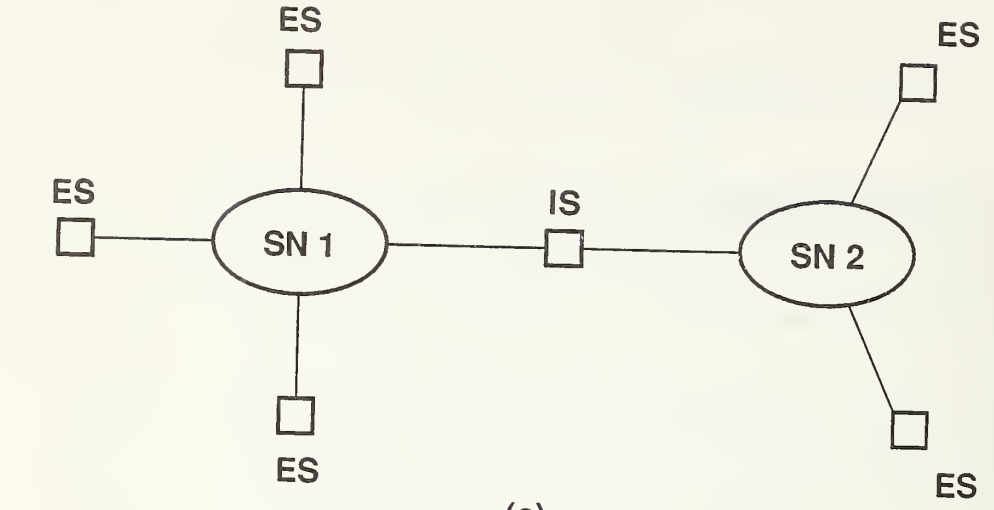
The NSAP (Network Service Access Point) addressing structure incorporates various numbering schemes or types of addresses to deal with the diverse users of packet data. The NSAP address consists of two major parts, the Initial Domain Part (IDP) and the Domain Specific Part (DSP) (see fig. 17). The IDP is subdivided into two parts which are specified by ISO 8348/Addendum 2.

The first part, Authority and Format Identifier (AFI), identifies the type of address being used and gives the syntax of the DSP. GOSIP uses a format defined by ISO 6523 ICD (mentioned previously) and a

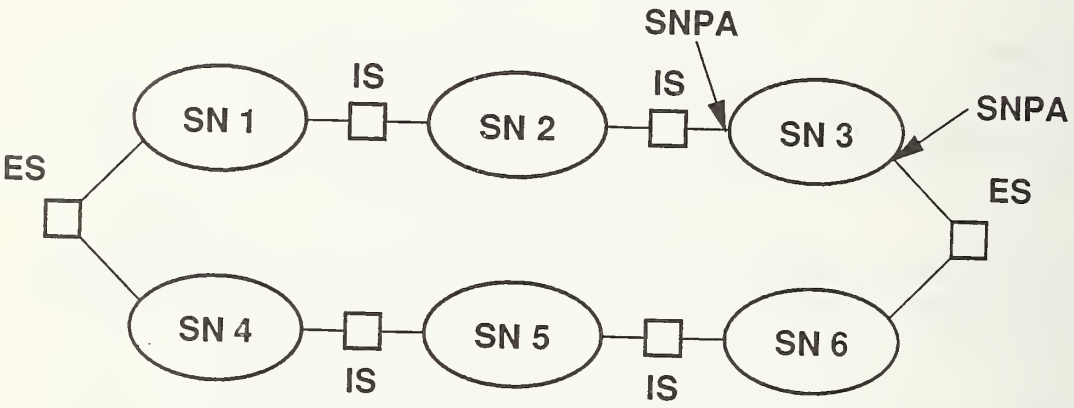


ES = END SYSTEM
PC = PERSONAL COMPUTER

FIGURE 15
END SYSTEM EXAMPLES



(a)



(b)

SN = SUBNETWORK
ES = END SYSTEM
IS = INTERMEDIATE SYSTEM
SNPA = SUBNETWORK POINT OF ATTACHMENT

FIGURE 16
INTERMEDIATE SYSTEMS AND SUBNETWORKS

binary syntax for the DSP. This is signified by an AFI value of 47.

The second part, Initial Domain Identifier (IDI) specifies the domain to which the address belongs. The IDI value of 0005 represents the domain which has been assigned to the U.S. Government. GOSIP systems must be able to communicate with systems which use other IDI formats and syntaxes as well.

The format of the DSP is not defined by ISO 8348/Addendum 2, but must be established by the registration authority for the 0005 domain. The format used in GOSIP Version 2 is illustrated in figure 17. The standard allows a maximum length of 20 octets for the NSAP and this has been allocated as shown in figure 17. Although technically, today, the 17-octet DSP shown in figure 17 is a violation of the base standard, an addendum is progressing through ISO to allow full conformance of this DSP format to the standard.

In figure 17 the AFI of 47 occupies one octet, and the IDI of 0005 occupies two octets. These two values are encoded as binary coded decimal digits. One octet is allocated for the DSP Format Identifier (DFI), three octets for the administrative authority identifier, two octets for routing domain, two octets for area, six octets for end system identifier, and one octet for NSAP Selector. Note that two octets have been reserved for expansion.

The DFI field identifies the version of the DSP structure and associated semantics encoded within an NSAP address. The DFI value 80H has been assigned to the NSAP structure as defined in GOSIP Version 2.

To understand the format of the DSP, think of each system as being in one or more network addressing or administrative domains. An administrative domain is defined by ISO as a collection of end systems, intermediate systems, and subnetworks operated by a single organization or administrative authority. These domains may or may not be synonomous with organizational entities.

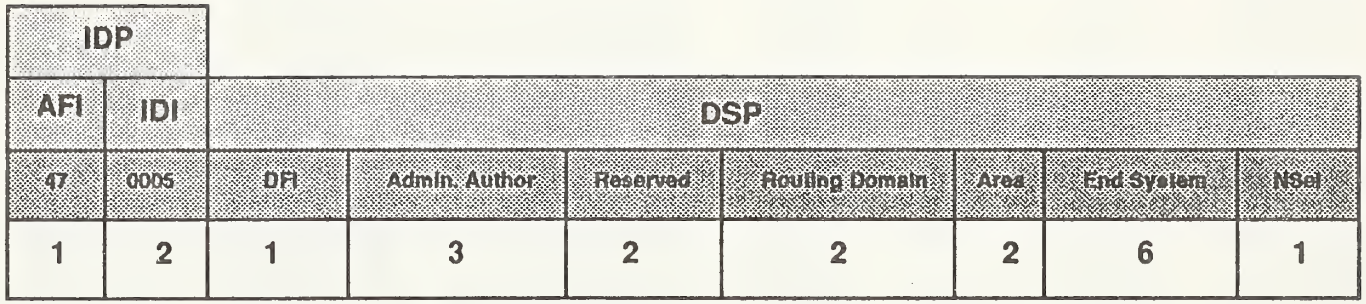
Within an administrative domain there may be zero, one, or more routing domains. A routing domain is a set of end systems and intermediate systems which operate according to the same routing procedures and which is wholly contained within a single administrative domain. Systems within a routing domain possess the following properties: (1) a high degree of trust in exchanging routing information with other such systems, and (2) use of the same routing protocols as other such systems. These properties may not be present in systems outside this routing domain. A routing domain is divided (usually partitioned) into subdomains called areas. A minimal amount of routing information needs to be transferred between adjacent areas in order to determine the most appropriate path to a system within a particular area.

The system ID field identifies a unique system within an area. The value of the system ID field may be a physical address (i.e., SNPA address) or a logical address. In the latter case, a locally administered table will be used to map the logical address to a corresponding physical address. Once the end system is found, the directional routing stops; now all that remains is to find the appropriate user of the network layer service within that end system. This is done by examining the value of the NSAP selector field. The NSAP selector field identifies the user of the Network Layer service, usually a Transport entity.

As an example, suppose that an agency system receives the following NSAP: 47 00 05 80 32 12 00 00 00 53 18 44 27 22 22 22 22 22 22 01 (hexidecimal)

This heximecimal NSAP will be interpreted as follows:

AFI==47
IDI==00 05
DSP Format Identifier==80
Administrative Authority Identifier==32 12 00
Reserved==null
Routing Domain==53 18



Legend:

AFI - Authority and Format Identifier
IDI - Initial Domain Identifier
IDP - Initial Domain Part
DSP - Domian Specific Part
NSAP - Network Service Access Point
DFI - DSP Format Identifier

Figure 17
U.S.Government NSAP Address Structure

Area==44 27
End System==22 22 22 22 22 22
N-Selector==01

8.3.3 Transport Service Access Point (TSAP) Selector

A TSAP selector identifies a point within a computer system where information is passed in both directions between the Transport Layer and the Session Layer. The TSAP selector does not have to be unique globally, but must be unique within an end system; it is appended to the NSAP address (forming a TSAP address) to identify a user of the Transport service. There may be more than one TSAP selector per end system; each identifies a separate user of the Transport service.

The TSAP selector has meaning only within an end system. The TSAP is encoded as two binary octets. Values can be assigned for the TSAP as long as they are the correct type and format (see sec. 5.2 of the GOSIP FIPS), and are interpretable by the destination end system. If a particular TSAP selector of one end system must be known to another end system, that value could be conveyed a priori or by a common directory service.

8.3.4 Session Service Access Point (SSAP) Selector

The SSAP selector is two octets, and identifies a point in the system through which information passes in both directions between the Session Layer implementation and the Presentation Layer implementation (see sec. 7). The SSAP selector identifies a user of the Session service. There may be more than one SSAP selector per end system; each would identify a different user of the Session service.

Any value may be inserted for the SSAP selector as long as it is the correct type and format (see sec. 5.2 of the GOSIP FIPS), and is correctly interpretable at the other end system. In transmitting information the SSAP selector is appended to the end of the TSAP address (forming an SSAP address). If it is necessary for one end system to know the SSAP selector for another end system, then that information could be conveyed a priori or via a common directory service.

8.3.5 Presentation Service Access Point (PSAP) Selector

The PSAP selector identifies a user of the Presentation service in an end system. The PSAP selector does not have to be globally unique. PSAP selectors are encoded in Abstract Syntax Notation (ASN.1) type OCTETSTRING. There may be more than one PSAP selector per end system; each value identifies a different user of the Presentation service.

Any value may be inserted for the PSAP selector as long as it is the correct type and format (see sec. 5.2 of the GOSIP FIPS), and is correctly interpretable at the other end system. If it is necessary to identify a PSAP selector on one end system to another end system, a common directory service could be used, as well as an a priori method. A PSAP address consists of the PSAP selector appended to the SSAP address, and is intended to globally identify an application.

8.4 Organization Names

8.4.1 Background and Importance

Organization Names (Names) are assigned by a registration authority for use in MHS X.400 (1984) O/R Names. For convenience of use, Names should be as short as possible, while still conveying the identity of the organization. For GOSIP users, Names will consist only of alphabetic and numeric characters. The special character "+" may be used in certain cases to construct Private Management Domain (PRMD) names, as described in section 8.4.2.

8.4.2 PRMD Names

It is assumed that most Government agencies will have access to an Administration Management Domain (ADMD). For example, this might be one of the providers of FTS2000 packet switched service (see section 10.2.1). If the agency uses ADMD services for delivery of electronic mail to the agency's PRMD, then the PRMD must register its PrivateDomainName with the ADMD. The agency will probably wish to register the same Name with GSA as well as with the ADMD. If a PRMD is connected directly to another PRMD under a bilateral agreement, then the AdministrationDomainName attribute will be blank, represented by a single space.

If the AdministrationDomainName attribute is blank, then the PrivateDomainName becomes the top level name under CountryName and should be unique within the United States. Registration of a Name with GSA IS NOT a guarantee of such uniqueness since other registration authorities will be assigning names at the same level.

In order to achieve a high degree of certainty that a PrivateDomainName is unique, agencies may construct it using the following syntax:

GOV+Name

"GOV" is an identifier which has been registered with the American National Standards Institute (ANSI) for use within the U. S. Government. The "+" sign indicates that the name has been constructed using a registered Name. The Name is one registered with GSA. Therefore, a PrivateDomainName might be constructed as: "GOV+GSA". Agencies are free to use the construction syntax as necessary without additional applications for registration. The limit of 16 characters, including "GOV+" (four characters), applies.

Although the construction syntax is generally adequate for Government needs, it is not an absolute guarantee of uniqueness. Agencies needing guaranteed uniqueness for a PrivateDomainName should register it with a U.S. level registration authority, such as ANSI. As of this writing, the final ANSI registration procedures have not been published. Agencies needing information on how to register with ANSI may contact the GSA Telecommunications Customer Requirements Office [MISC 6].

8.5 Application-Specific Object Registration

The second group of objects to register for the GOSIP FIPS includes (1) FTAM document type names, (2) MHS private body parts, and (3) virtual terminal (VT) profiles and control objects. In general, registration of FTAM document types, MHS provate body parts, virtual terminal profiles and control objects, and document application profiles is completed by standards groups or implementation workshops. Thus, such registration for GOSIP should only be requested under special circumstances.

8.5.1 FTAM Document Type Name

Document types in FTAM are descriptors of the structure, syntax, and semantics of a file. This information is separate from the file contents itself; it tells how the records and blocks of data that constitute a file are organized, as well as how long each record or block is, and the range of data types that are possible in the file contents. For example, a file could be a single binary file of length 10000 bits, or it could be a sequence of 200 fixed-length records of 50 ASCII characters each, with CR (carriage return) and LF (line feed) symbols separating the records. Each of these is a different document type, and so has a different document type name.

This document type information must be passed between two FTAM implementations (using the FTAM protocol) to enable each implementation to anticipate properly what will be transferred and to accommodate the data when it is transferred. Thus it is important to register document types and their names.

Some document types are already registered. Some are defined in the ISO FTAM International Standard and some are defined in the NIST Workshop Agreements. These generic document types have been defined

because they represent file structures that are widely used and easily described. Note that the names of document types in the NIST Workshop Agreements have been changed in the December 1989 NIST agreement because the previous names were ad hoc names chosen in the absence of official registration authorities.

Agencies may have unique file structures that do not conveniently fit into any of these defined document types. If agencies plan OSI communication with other agencies using these unique file descriptors, then they should be registered with the GSA to ensure unique document type names. If communication is within an agency, then registration with the GSA is not necessary, but procedures should be in place within that agency to make sure that the document type information is understood and interpreted correctly. In any case, these document types must have unique names that are not used for any other document type by any other implementor. The existing document types should be used by agencies whenever possible; these will cover most file types of interest to Federal agencies.

8.5.2 Private Message Body Parts

A message body part number describes the form and syntax of the data being transferred. All MHS implementations are required to be able to generate IA5 text body parts. MHS vendors will specify if additional body part types are supported by their implementations.

The CCITT X.400 Recommendations Series defines 12 generic body part types. These pre-defined body part types should satisfy Federal requirements for transferring MHS information. In exceptional instances, Federal agencies may require the assignment of special body part numbers to communicate special messages to other agencies.

8.5.3 Virtual Terminal Profiles and Control Objects

Implementation of the Virtual Terminal standard may require registration of some terminal profiles and control objects. A terminal profile is a complete and consistent set of parameters relating to a particular type of terminal (e.g., VT 100). Default profiles in the NIST Workshop Agreements will satisfy most user requirements, thus user registration of separate terminal profiles is not normally needed.

Control objects are used to transfer terminal information that refers to "value added" features that are specific to a terminal type An example is a control object which provides a sophisticated coloring capability for graphic terminals. An agency may have requirements beyond those specified in the NIST Workshop Agreements.

8.5.4 Other Registration Objects

This guide has covered common objects which must be registered or are likely to be registered under GOSIP. Other objects may need to be registered now or in the future. An abstract syntax is one of these. An abstract syntax is the notation that an application uses to represent, encode, and transmit data structures. One such notation is called Abstract Syntax Notation One (ASN.1). The format of the encoded bit stream is called the transfer syntax, and this must be registered as well. Examples of abstract and transfer syntaxes can be found in the Implementation Agreements for FTAM.

Application contexts must also be registered. An application context is a detailed specification of the use of an association or connection between two open systems. In OSI, the communications capabilities of open systems are organized into groups of related capabilities called Application Service Elements (ASEs). The ASEs are defined for a particular purpose, and identified by application contexts. In the 1988 CCITT X.400 Recommendations, the application context which describes access to the message transfer system, uses message handling ASEs for submission, delivery, and administration, and is represented by the P3 protocol. This and other application contexts are registered in the X.400 Series of Recommendations. An example of an application context is "ISO FTAM"; each ASE may be represented by one or more application contexts.

Application entities and application processes need to be identified by titles. An example of an appli-

cation process in MHS is a MTA. Such a process includes a user element, which defines the role or process to be that of a MTA. and the ASEs that the MTA needs in order to play its role of message submission or transfer.

Managed objects are another category of objects which will need to be registered. The network management standards and implementation agreements are in process and will register managed objects. Rules for registering network management objects will be included in a future version of GOSIP.

Another category that will be registered in the future is that of Relative Distinguished Names in directories. As an example, each person under an Organization will be registered as a Relative Distinguished Name under that Organization. This will follow the hierarchy originating with ISO 3166 Country Codes which was mentioned earlier. A directory enables users to identify, understand, and locate objects within the network. These actions are accomplished through names, attributes, and addresses, respectively. The user supplies to the directory service a Relative Distinguished Name. The directory service returns a set of attributes corresponding to the name.

8.6 Detailed Procedures for Registration

The NIST has delegated to GSA the authority to assign values for NSAP Administrative Authority Identifiers (AAIs) under ISO 6523 iso (1) identified-organization (3) ICD (5) (see section 8.2), X.400 Organization Names under identifier "GOV", and Technical Objects under ISO 3166 iso(1) member body(2) US(840) GOV(101) technical objects(0). The AAI unique numbers will start with 256 in decimal or "000100" in hexadecimal. In a technical registration, a definition of an object is necessary along with the identification of the object. The numbers for technical objects will be assigned in a subarc under registration number 0 decimal.

For more information on detailed registration procedures, refer to the GSA GOSIP Registration Services Document [MISC 6]. No GOSIP registration service for technical objects (see sec. 8.5) is available as of May 1991; such a service is possible in the future. Consult GSA for details.

8.7 Summary

In summary, for the GOSIP FIPS, the OSI objects to be registered are the NSAP Administrative Authority Identifier, X.400 Organization Name, FTAM document type name (optional), MHS private body part (optional), and virtual terminal profiles and control objects (optional). In addition, application contexts and application entity titles should be registered by Federal agencies when there are agency-specific requirements for definitions for these objects. It is important to register these objects in order to provide unique identification for OSI communication in a GOSIP environment. To register identifiers, users should refer to the GOSIP Registration Services Document [MISC 6], published by GSA.

Users should read and understand this information. Registration information is also found in section 5 of the GOSIP FIPS.

9.0 GOSIP TRANSITION STRATEGIES

9.1 Introduction

GOSIP creates an opportunity for each Federal agency to assert control over future procurement. Adoption of GOSIP as a long-term strategic initiative will lead to evolution of current systems into a GOSIP-compliant interoperable set of computers within that agency. What follows is some general advice concerning a transition towards GOSIP-based networks, which will provide the benefits to agencies that have been previously described.

In this section, recommendations for transition strategies will be given and specific alternatives will be proposed based upon an agency's particular requirements. It should be emphasized that the information in this section is only a guideline. It is up to the procurement and technical authorities in each office to make the proper decisions on transition based upon their own particular situation.

Each of the subsections below offer a different perspective on the OSI transition problem. Agencies may want to adopt more than one solution for different components of ADP systems. A higher level of integration will then take place combining each of these proposed solutions. The end result is a GOSIP-based internetwork. As current systems reach the end of their life cycles, they should be replaced by GOSIP-compliant systems.

Section 9.2 gives a generic course of action for Federal agencies in transitioning to GOSIP systems. Agencies may currently find that one of two possibilities exists as follows: (1) current architectures map conveniently into the OSI architecture, and (2) there is no convenient mapping between current architectures and OSI architectures. Figure 18 gives an illustration of each of these two possibilities. These two possibilities will lead Federal agencies to different courses of action.

When the architectures map conveniently, suggested strategies to follow are described in section 9.3. Section 9.4 elaborates on actions when the architectures do not map. Section 9.5 describes strategies for interoperability with non-GOSIP OSI systems. General considerations for transitioning to OSI systems are given in section 9.6, and finally, a brief summary follows in section 9.7.

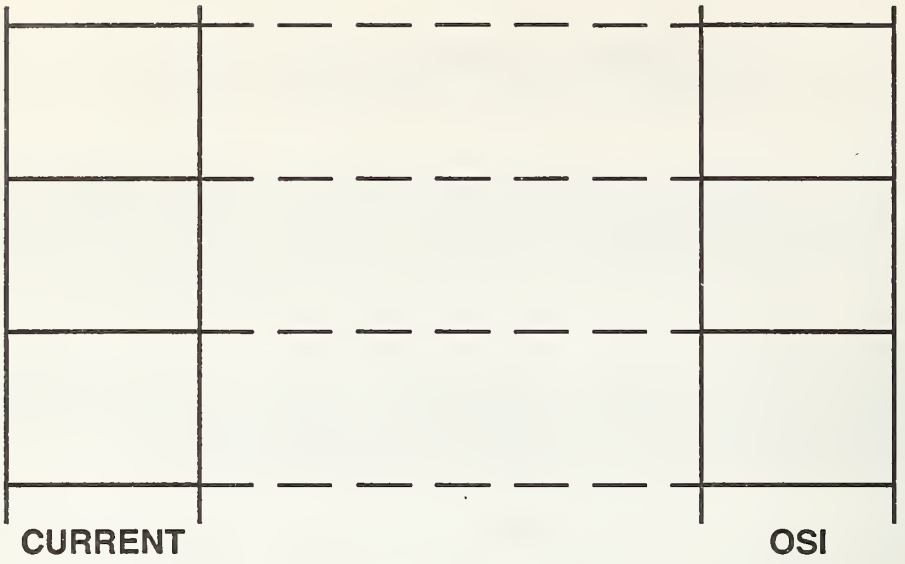
In transition to GOSIP systems, a comprehensive transition plan must be devised as soon as possible, and policy makers within an agency should coordinate acquisitions to take account of all of the factors that are important to correctly assimilate OSI technology into the Federal environment. Vendors and users should discuss how these strategies will be implemented in particular situations.

9.2 Perspective on the Process

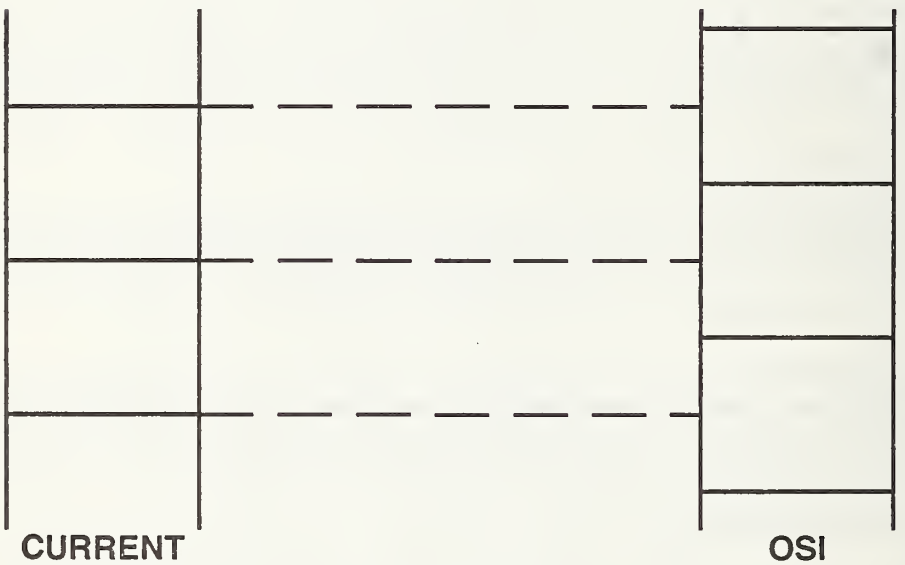
The single most important recommendation for an agency is that a clear and definitive policy be established concerning the adoption of GOSIP. Such a policy serves several goals. First, a clear and definite signal is sent to agency operating components that a future networking direction has been set. The operating units can then begin to plan seriously for transition, knowing that agency backing is assured. Network suppliers are also put on notice that the agency is going in the direction of GOSIP. These vendors can then reorient their marketing strategies accordingly.

Having announced a clear policy, an agency should require that each affected operating unit prepare a transition plan indicating the time goal and mechanisms for implementing the policy. Intelligent planning for, and adoption of GOSIP will pay dollar benefits over the long term. However, it is unrealistic to expect an operating unit to adopt the provisions of GOSIP at an inappropriate point in the life cycle of its systems. Adoption of GOSIP should be coordinated with plans for replacing or upgrading major computer and network systems.

Once a transition plan is in place, orderly implementation of interoperable computer networks can begin. Implementation will involve the procurement process, the network design process, and education of users



a) SIMILAR



b) DISSIMILAR

FIGURE 18
FUNCTIONAL LAYER MAPPINGS TO OSI-TWO SCENARIOS

and consultants within the agency. This strategy is being successfully applied by the DOD and DOE to implement OSI, and it is likely that it can be successfully applied by other agencies as well.

An agency should (1) examine where it is now with respect to OSI technology, (2) determine where it wants to go, and (3) determine how to get there (i.e., via a series of steps or stages). Each alternative should be examined to determine what is most appropriate for that agency. Following this, a decision should be made on which strategy is best, and the appropriate recommendations should be made and implemented in acquisition plans. Agency policy with respect to life cycle management must be integrated into these decisions (e.g., duration of the cycle, components of the cycle). Resource materials on OSI (including this Guide) should be extensively consulted.

Given that an agency has vendor-specific configurations, several decisions must be made as follows: (1) an agency must develop a procurement strategy in accordance with the instructions in section 6 and (2) an agency may consider applicability and waiver procedures (as described in sec. 5).

Vendors will make suggestions as to how to provide a smooth transition to OSI while preserving capabilities inherent in their particular user interface during the OSI transition process. The vendor whose architecture differs radically from OSI is likely to emphasize the private architecture approach while offering gateways to OSI products. On the other hand, the vendor whose private architecture is close to that of OSI is more likely to effect a smooth transition to a total OSI solution; in this case, private architecture solutions will have a limited life.

9.3 The DOD Approach

The Department of Defense (DOD) has taken a leading role in the evolution of networking. The Defense Advanced Research Projects Agency (DARPA) has been instrumental in network research. A major network within the Defense Data Network (DDN), MILNET, is an operational deployment of the technology pioneered by DARPA. There are many organizations in the Federal Government (civilian and military) that use the MILNET and other interconnected networks.

The DOD issued a three-page policy statement in July 1987 announcing plans to adopt the GOSIP FIPS and to begin transition of the DDN to GOSIP protocols. In June 1988 the DOD issued a plan for implementing the policy. Several independent agencies of the DOD are procuring GOSIP products to gain operational experience. Other components are permitting vendors to offer either GOSIP or DOD protocols. The DDN backbone plans to move toward complete use of the GOSIP protocols by 1993.

The DOD has investigated OSI transition and interoperability issues extensively and the approaches taken by the DOD are deliberately generic. Accordingly, any of the DOD approaches to transition may be used in other situations and in other environments, particularly when there is a functional equivalence between existing architectures and the OSI architecture. For DOD, the OSI protocols are the sole mandatory interoperable protocol suite for new DOD acquisitions; however, a capability for interoperation with DOD protocols will be provided for the expected life of systems supporting the existing DOD protocols.

The transition from DOD to open systems is concerned with both implementing OSI and providing interim DOD/OSI interoperability until OSI implementation is complete. Implementation deals specifically with deploying open systems products and services in existing or future DOD networks. Interoperability provides a capability for the military standard protocols on existing DOD networks to interoperate with the open systems protocols being produced. DOD will support the existing protocols for the expected life of the systems using them. By moving to OSI protocols as the means for computers to interoperate in DOD, the potential for interoperability with comparable open systems used by NATO (North Atlantic Treaty Organization) is greatly increased.

The DOD approach to transition is multi-faceted, including: (1) developing a full stack of OSI protocols in a portable operating system environment (ISODE and POSIX (for both, see sec. 9.3.1)), (2) having both protocols co-exist on a particular host (dual-protocol host), (3) converting from one Application-Layer

protocol to another (Application Layer gateway), (4) supporting both DOD IP (Internetwork Protocol) and CLNP at the Network Layer (multi-protocol routers), and (5) establishing a DMS (Defense Message System) project to develop and implement plans for transitioning to the CCITT Message Handling Systems; each of these has advantages and disadvantages, and all may have particular importance in a variety of situations. An example internetwork scenario showing some of these methods is given in figure 19.

The DOD is requiring services and agencies within its purview to develop specific implementation plans incorporating many of the above concepts. Experience gained in incorporating GOSIP functionality into large DOD programs such as CALS (see sec. 10.2.7) and the DMS (Defense Messaging System) should prove invaluable.

9.3.1 ISODE and POSIX

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

The ISODE (ISO Develpment Environment) is a UNIX-based public domain software package that includes the OSI Application, Presentation and Session Layers. The ISODE runs over the OSI lower layers, but it also contains an interface which allows the OSI upper layers to "run" over the TCP (Transmission Control Protocol). Using this interface, OSI applications can run in a DOD networking environment using DOD hosts. The disadvantage of this approach is that an end system can communicate only with end systems that have the same mixed protocol stack; however, this alternative may be useful as a research or education tool during the transition period. The ISODE software includes the MHS, FTAM, Directory Services, and VT applications, and is available by "anonymous FTP" to host "nisc.nyser.net", or by writing to: University of Pennsylvania, Department of Computer and Information Science, Moore School, ATTN: David J. Farber (ISODE Distribution), 200 South 33rd Street, Philadelphia, PA 19104-6314.

POSIX (Portable Operating System for Computer Environments) is a standard application interface for UNIX-like operating systems. Efforts are underway to put additional functionality into ISODE and to make ISODE POSIX-compliant. A POSIX FIPS [NIST 4] gives Federal requirements; non-UNIX operating systems may be POSIX-compliant.

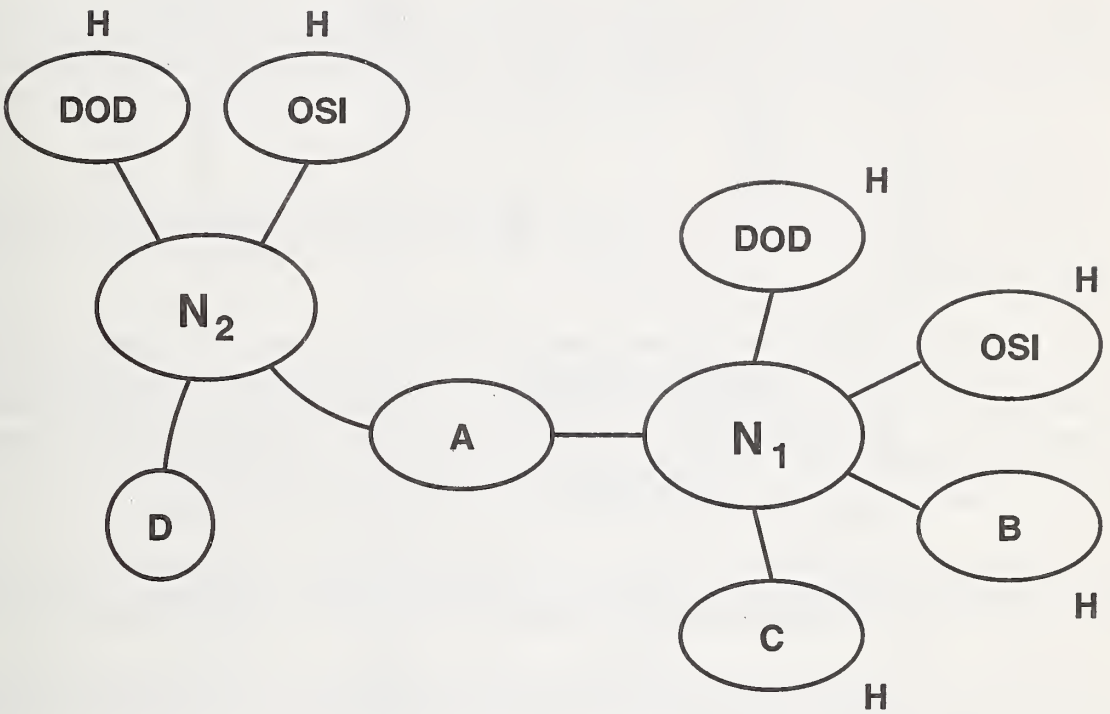
A continuing goal is to disseminate an implementation of the OSI protocols to the academic and research communities that use Berkeley UNIX. In addition, the Berkeley UNIX OSI software serves as a reference implementation for GOSIP testing. With POSIX-conformant OSI protocols, as well as anticipated POSIX extensions to define an interface for network services, application software written to use OSI services could be much more portable.

9.3.2 DOD-OSI Multiprotocol Routers

In order for DOD-OSI internetworking to occur, it is necessary to provide OSI hosts, on a local area or wide area network, the ability to communicate with other OSI hosts on another DOD-based local area or wide area network. Since the DOD IP and OSI CLNP are similar in functionality and protocol structure, multiprotocol routers are a viable alternative. The availability of multiprotocol routers would reduce the number of components, and therefore presumably reduce the cost and complexity for DOD LANs that are composed of a mixture of DOD and OSI protocol hosts, allowing the use of DOD protocols in areas in which OSI protocols are not yet mature (e.g., internetwork routing and network management).

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

9.3.3 Dual Protocol Hosts



A = MULTI PROTOCOL ROUTERS
B = APPLICATION - LAYER GATEWAYS
C = DUAL - PROTOCOL HOSTS
H = HOST
N_n = NETWORK $_n$
D = DUAL - PROTOCOL TERMINAL
ACCESS CONTROLLERS

FIGURE 19
DOD TRANSITION APPROACHES

A dual protocol host has the complete OSI and DOD protocol suites available as part of its networking capabilities. A user of such a host would have the option of invoking the DOD protocols (TELNET for remote login, FTP (File Transfer Protocol) for file transfer, and SMTP (Simple Mail Transfer Protocol) for electronic mail) or the analogous OSI application protocols (VTP for remote login, FTAM for file transfer, and MHS for electronic mail).

A dual protocol host can be used directly by users with accounts on it to communicate to any OSI or DOD destination. It can also be used as a staging point for manual interoperation between a host that has only DOD protocols and a host that has only OSI protocols. A user on a host that has only DOD protocols could transfer a file to a host that has only OSI protocols by using a dual protocol host as an intermediary.

9.3.4 Application-Layer Gateways

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

The OSI File Transfer (FTAM) and Message Handling (MHS) protocols (sec. 7) are candidates for such a gateway. The NIST has developed and tested prototypes of a gateway connecting the DOD SMTP and the OSI MHS protocols, and a gateway connecting the DOD FTP and OSI FTAM protocols; documentation is available [NIST 5-6]. The NIST also plans to provide an MHS-SMTP gateway as an FTS-2000 service (see sec. 10.2.1). The NIST effort demonstrates the viability of a relatively efficient means of interoperation between systems based on the Transmission Control Protocol (TCP) and OSI-based systems.

The gateways were designed so that users require minimal knowledge of the remote protocol, as much capability as possible is retained for each protocol, and the protocols being converted are not modified. Figure 20 illustrates how the SMTP-MHS and the FTP-FTAM gateways would look schematically.

Some agencies may have a requirement for dial-up access supporting the OSI Virtual Terminal (VT) service with the Telnet profile. This requirement may be implemented as a VT gateway. The DOD is encouraging commercial offerings in this area.

9.3.5 Dual Protocol Terminal Access Controller

Dual protocol terminal access controllers are terminal servers supporting dial-up access; these servers enable users to specify OSI or DOD hosts remotely, via their respective terminal characteristics. Remote login would be accomplished through TELNET (for DOD hosts), or VT (see Appendix A) for OSI hosts; both protocols are supported in the controller. Such controllers provide a convenient means of allowing operation on either DOD or OSI hosts across a network.

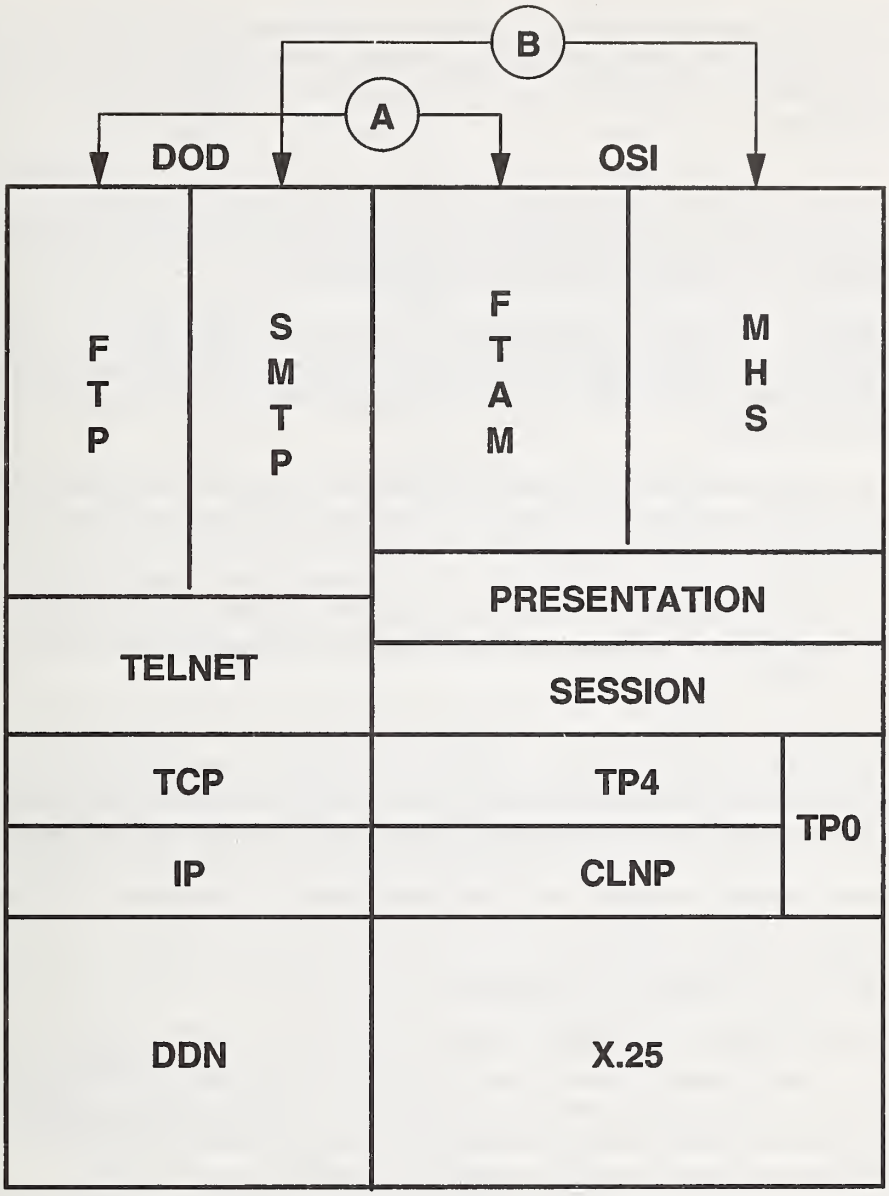
9.3.6 Defense Message System

The Defense Message System will be the organizational and personal messaging system of the DOD, and will be based on the 1988 CCITT MHS Recommendations, enhanced by the use of the Message Secure Protocol (MSP) for security and integrity. The DOD will transition the AUTODIN and INTERNET messaging systems to the Defense Message System in three phases (concluding in the year 2008), while maintaining operational capability during the transition.

9.4 Other OSI Transition Concerns

The second class of existing architectures, as mentioned previously, do not map conveniently to the OSI architecture. The choice of alternatives to use represent implementation decisions that should be made by the vendors. Users should concentrate on stating their functional and performance requirements.

Users choose interoperability solutions based upon an understanding of end-user requirements; these



A = FTAM - FTP GATEWAY
B = MHS - SMTP GATEWAY

FIGURE 20
GATEWAY ARCHITECTURAL MODEL

requirements are evaluated on such factors as the level of interoperability required, the range of vendor(s) equipment to connect, the cost to implement and maintain, and the implementation schedule requirements. In addition, the degree of network management required and supported is a significant factor in providing reliable service to the end user.

Other concerns for interoperability involve: (1) the sharing of hardware resources such as terminals and communication links, and (2) support for interoperation of a basic set of application functions. In addition, there is the need for application-to-application interoperation. Important components of study include: identifying functional layer incompatibiities, and address mapping issues.

The most comprehensive and simplest interoperability is achieved by implementation of equipment conforming to a single full-function networking architecture. For environments involving multiple vendor architectures, a compromise may exist between the level of interoperability achieved and the number of vendor environments to be supported.

Terminal protocol converters or emulators provide an inexpensive and effective interoperability capability for single architecture networking environments. Gateways may be optimized for performance but are difficult to extend to support additional vendors' environments.

Gateways may be a workable approach for interoperability between products of a small number of vendors (two or three). International standards provide the only workable approach for interoperability between a large number of different vendors.

Vendors whose architectures do not map conveniently to the OSI architecture may decide to provide gateways or protocol converters as a long-term solution, while (a) providing for a gradual transition to OSI, or (2) allowing both OSI and the existing native architecture to co-exist permanently. It is possible that special user services which exist in the native architecture will be preserved by the vendor; OSI will be available via special hosts or processors. As another approach OSI could be used to permanently interconnect two native architectures. Users should transmit to vendors any critical requirements in these areas, and allow vendors to develop specific responses to these concerns.

9.5 Interoperability With Non-GOSIP OSI Systems

A problem that Federal agency systems administrators must consider is that of communication with non-GOSIP OSI systems. This is primarily because many non-GOSIP systems use the CONS (Connection-Oriented Network Service) and Transport classes other than Class 4, whereas GOSIP-compliant systems are linked by the CLNP (Connectionless Network Protocol) and Transport Class 4. To effect the required interworking, Federal agencies may have to employ procedures outside the scope of GOSIP.

There have been several interim measures proposed to handle this incompatibility, including: (1) a "265" interworking function, (2) a DSG (distributed systems gateway), (3) a MSDSG (multi-system DSG), and (4) an Application-Layer gateway. All have some disadvantages and advantages, and are discussed in a MAP/TOP Position Paper [MISC 4].

The "265" interworking solution is a Network relay that uses the connection-oriented and connectionless network services to relay data between Transport Class 4 processes. Since Transport Class 4 must be used at both ends of the Transport connection, this solution has little support in the connection-oriented community, which typically uses Transport Class 0 or 2.

In the DSG approach, a Transport Layer relay is used to provide the inter-working between connection-oriented and connectionless end systems. This approach is viewed by some to be a violation of the OSI architecture, which expressly forbids Transport Layer relays. This approach is viewed by others to conform by considering the connection-oriented environment as a single large OSI system when viewed from the connectionless environment and vice versa. Other profiles (e.g., U. K. GOSIP) may select this approach as a bridge between local area and wide area networks.

The MSDSG approach is a variation of the DSG which simplifies NSAP addressing. Neither the DSG or MSDSG approach places any restrictions on the class of Transport that is used by GOSIP and non-GOSIP OSI systems. Since the same class of Transport cannot be assumed, end-to-end security mechanisms that rely on a particular class of Transport or hop-by-hop security relying on the CLNP cannot be assured. None of these three approaches has been widely implemented. Users should consult with their vendors for additional security information.

In contrast to the other three approaches, the Application Layer gateway is architecturally correct and is particularly useful in the relaying of messages between Message Transfer Agents which use Transport Class 0 and the CONS, and those which use Transport Class 4 and the CLNP. (See Appendix A for additional information.) In addition, implementations of the Application-Layer gateway for this purpose (relay MTAs) are expected to be widespread. The Application-Layer gateway can also be used to implement security services at the Application Layer. For applications such as file transfer, virtual terminal, and transaction processing, Application-Layer gateways introduce inefficiencies that would not normally exist.

The best means of assuring interoperability across CLNP, CONS, and the most common range of Transport classes is the purchase of end systems capable of supporting all the required services. Many vendors serving the international marketplace offer Transport Classes 0,2, and 4 and also offer both CLNP and CONS. This solution will work well when an end system is connected directly to a wide area network supporting CONS. When end systems are attached to a local area network, where CONS is usually not supported, products containing only Transport Class 4 and CLNP are appropriate.

For communication with OSI-compliant non-GOSIP End Systems, it will be necessary for ISs to route to destinations in routing domains which use other addressing formats, such as those specified by ANSI or ECMA (European Computer Manufacturers Association). In this case, it will not be possible to ensure that the GOSIP address format is followed. Such interconnectivity will take place via inter-domain routing (i.e., routing domains using GOSIP addressing and routing procedures should not be expected to contain non-GOSIP ESs).

For inter-domain routing, it will therefore be necessary for ISs to be capable of routing PDUs to other domains, based on variable length administration/routing domain identifiers, specified as address prefixes. Similarly, it is necessary that end systems be able to deal with NSAP addresses for remote ESs as variable length octet strings, up to 20 octets in length, whose internal structure, beyond the initial domain identifier (IDI), is not interpreted directly.

9.6 General Transition Issues

The following general guidelines will serve to further assist users in making decisions relating to OSI, and in properly implementing the decisions that are made. These considerations apply to all of the information previously discussed, and are independent of any particular strategy selected. It is important for vendors and users to work out mutually acceptable agreements regarding a particular agency and OSI. Users should give any functional and configuration requirements, and vendors should attempt to suggest and design optimal specific solutions for particular user concerns.

Considerations are divided into the following categories: general (architectural), and user-related. These are presented below.

GENERAL (ARCHITECTURAL) ISSUES

These issues deal specifically with configuration or architectural considerations.

(1) Some questions are : (a) will the vendor migrate to OSI from its native environment?; (b) will compatibility between phases be maintained?; and (c) will gateways play a role in the vendor's long-term strategy?

(2) Other questions are: (a) does the vendor have an OSI migration plan for customers?; (b) can existing applications be protected in the transition to OSI?; and (c) can both proprietary and OSI protocols be supported in initial OSI offerings (e.g., in all products or just selected ones)?

(3) It is important to determine if communications between an OSI product and a proprietary product will be supported, and if previous releases of the vendor's proprietary network products will work with new OSI releases.

(4) The vendor should have an OSI migration plan for customers. Where possible, compatibility between phases should be maintained. The schedule for the availability of OSI products within the context of the transition should be available.

(5) Are user interfaces to the network the same for both OSI and proprietary products, or are there different interfaces for each category?

(6) It is primarily a vendor choice as to whether an OSI implementation can be integrated with their user interface.

(7) There may be a number of proprietary functions that are not provided by OSI systems. There could be a loss of functionality if mapping between vendor proprietary systems and OSI systems occurs. Users should be conscious that some loss of proprietary application functionality may occur with introduction of OSI products.

(8) How will access be supported to wide area networks? Will both OSI and proprietary networks use (a) X.25 packet switching, (b) X.21 circuit switching, (c) leased-lines, point-to-point, and (d) ISDN? How will access be achieved (host directly connected to wide-area network or via an intermediate system)? See section 7 for additional information on these topics.

(9) If a vendor is making the transition from a proprietary protocol stack to OSI, the layer at which the conversion takes place may vary. In the transition, conversions could be performed at the link layer (bridge), network layer (intermediate system), and application layer (gateway).

(10) A vendor could migrate to OSI and abandon proprietary products, or maintain both OSI and proprietary products. OSI capability could exist across all product lines, or just a subset (hardware and software); also OSI capability may exist on all systems or just selected nodes.

(11) Will OSI-proprietary communication be transparent to user applications? Will this function be integrated with the operating system?

(12) Vendors should be encouraged to limit the number of embedded interfaces in hardware and software. This provides for flexibility in accommodating future enhanced OSI functionality.

(13) There is no requirement to provide OSI application software in all U.S. Government personal computers; there are other methods of making these services available to the end user. This does not preclude vendors from offering and users from implementing OSI protocols within personal computers.

(14) What portion(s) of the network are considered homogeneous (in terms of network equipment, end systems, etc.)?

(15) Are there any time critical applications running on the network? What are the requirements for preserving display management semantics?

The suggestions described below deal with user issues in planning and developing a transition strategy. These issues should be discussed with vendors, but users have primary input.

(1) Cooperation of vendors should be solicited in developing a transition strategy; vendors can provide helpful suggestions as to how the move to OSI may best be achieved.

(2) Vendors should provide the same levels of functionality and service during a transition as before. Impact on user applications should be minimized.

(3) Not all Federal agencies need to communicate with other Federal agencies. Reasonable and prudent requirements for intra-agency and inter-agency interoperability should be determined and discussed with vendors.

(4) Not all transitions can be smooth. Short-term efficiency may need to be sacrificed for growth over the long term.

(5) It is important to keep subnetwork types consistent if possible, and to minimize the number of different kinds of networks involved in the transition. This will reduce the amount of work required to effect a transition.

(6) Modularize and isolate key network components in developing a transition plan. Identify the components that must be changed or procured.

(7) The practical impact on the network during upgrades should be considered (i.e., will all nodes be required to upgrade at the same time, and what will the total "downtime" be?)

(8) An implementation task force should be appointed. This task force should include individuals knowledgeable in the areas of the standards being referenced.

(9) A specific transition plan to OSI should be developed, with steps and dates included.

(10) It is important to keep future requirements in mind when planning a transition strategy. Such a strategy should allow for incorporation of additional OSI products as they become available.

(11) Multi-vendor product availability is an important reason to move toward GOSIP-compliant systems as quickly as possible even though usage may be restricted in the immediate future.

(12) In the immediate future, it may be necessary to specify nonstandard solutions to current concerns (e.g., network management) while striving for standardization of these functions.

(13) Users should recognize that user and program interfaces to OSI services will likely be nonstandard into the foreseeable future; however, users should specify as much standardization as possible in procurement requests to maximize portability of data, people and applications software.

(14) Users should recognize that the plan a vendor provides may be influenced by the degree to which the vendor's architecture differs from the OSI architecture.

9.7 Summary and Strategies

An agency may use any of the strategies defined above to move to OSI systems and may use combinations of these strategies depending upon particular hardware and software configurations. These strategies are generic, and may be used to make the transition from any proprietary architecture to OSI. There are advantages and disadvantages to any particular strategy. These suggestions do not constitute an exhaustive list; there may be other approaches more suited to a particular agency's environment.

An agency should (1) examine long-term goals, (2) examine the advantages and disadvantages of each of the strategies given above, (3) determine which (if any) will be useful to an agency, (4) develop a specific transition plan based upon the strategies selected, and (5) develop an acquisition plan based upon the selected transition strategies. For large agencies, several strategies may be selected and it will be up to internal agency policy to coordinate the various transition strategies into an acceptable comprehensive transition strategy and acquisition plan. Factors to be considered in a transition strategy include cost, simplicity of implementation, and compatibility with current hardware and software design.

10.0 GOSIP CROSS-REFERENCE

10.1 Introduction

Developments are taking place which will help Federal agencies use information technology to accomplish their missions more efficiently and effectively. The GOSIP initiative, the subject of this Guide, is just one of a number of efforts aimed at reducing costs and increasing capability. To achieve maximum effectiveness, these efforts must be complementary.

The NIST has defined an Applications Portability Profile (APP) to record a complementary set of computer and communications standards and interim approaches that may be used to achieve data communications interoperability and software portability. The APP may lead to development of standard software interfaces across a range of computing services such as operating systems, networking, database, and graphics. The APP may benefit users by enabling standard software interfaces for computing and communications services to be referenced in future procurements. Figure 21 indicates the relationship of GOSIP to the APP effort.

Obviously, separate components of the APP should not conflict with each other in the final version. Still, while the profile is under development, it is important for Federal users to ensure that no inconsistencies exist when planning procurements relating to long-term ADP acquisition. In particular, GOSIP acquisitions and those involving other functional areas of the APP (such as database management, data interchange, and language development) should be examined for consistency at every stage of the procurement process. The purposes of this section are to show how GOSIP fits in with the other programs, and to give guidance to Federal officials on strategies to pursue in integrating GOSIP requirements with other requirements.

How can an agency best take advantage of these developments to fulfill its mission? The answer is that agency officials should (1) gain knowledge of each of the efforts described below (by consulting appropriate reference materials), (2) make a determination for each of these areas, whether or not this aspect of information technology fits with the agency's long-term ADP development strategy, and (3) if it does, then the agency should monitor the progress of each applicable program, and determine its impact, if any, on the work of their agency.

10.2 Interaction of Other Programs With GOSIP

Brief descriptions of programs affecting current and future Federal information processing procurements are given below. The relationships of these programs with GOSIP are also discussed.

10.2.1 FTS-2000

FTS-2000 is a Government-wide upgrade of the Federal Telecommunications System (FTS). The General Services Administration (GSA) is administering this program. FTS-2000 will advance the communications capability of the U.S. Government, by replacing physical equipment, providing value-added services, and including digital capability. Voice, data, and video transmission will be supported over a variety of physical media, including those supporting ISDN and those supporting a packet-switched environment. The intent is to integrate these various means of transmission in an all-digital environment.

Close cooperation between GOSIP procurements and FTS-2000 procurements should be maintained. Communications requirements for FTS-2000 are functionally similar to those referenced by GOSIP when the requirements intersect (e.g., X.25 and X.400). When procuring GOSIP-compliant systems, U.S. Government procurement officials should consider the basic telecommunications capability supplied by FTS-2000 as a connectivity adjunct to GOSIP. This includes in particular GOSIP "value-added" services.

10.2.2 EDI

EDI (Electronic Data Interchange) standards describe formats for orders, payments, shipments, billing,

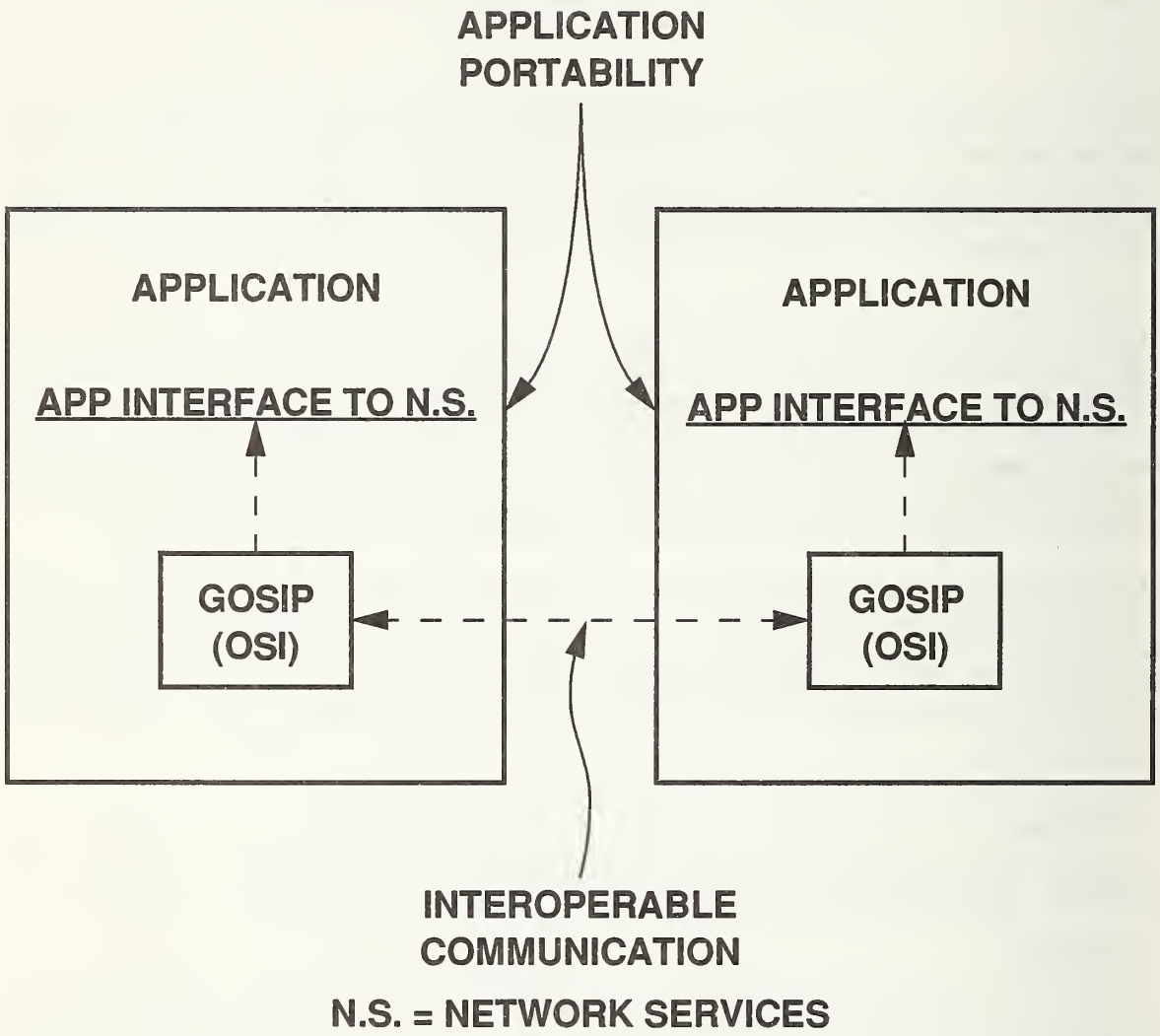


FIGURE 21
GOSIP AND THE APP

and other business transactions. It is widely used commercially, but is only starting to see Government use. There are two sets of standards for EDI, as follows: (1) the basic set, which contains interchange control, application control, data segment directory, and functional acknowledgement, and (2) transaction sets, which contain formatted messages.

The CCITT is working towards a standardized solution for exchanging EDI information using MHS. Two draft recommendations define the services and protocol required to accomplish this exchange. An EDI User Agent is planned for a future version of GOSIP.

In the interim, two approaches may be used to enable MHS to transmit EDI information; both approaches are based on extensions to existing MHS profiles. One approach specifies encapsulating EDI data inside an interpersonal message using the P2 protocol. The other approach allows EDI data to be transferred via the MHS as an "undefined" content type. A gateway may be used to link the two approaches.

10.2.3 RDA and SQL

Remote Database Access (RDA) is an emerging standard governing different access modes for a database model on a number of different systems. This model uses a structured database management system, which involves a data manipulation language called Structured Query Language (SQL). This language governs access to relational data bases. Extensive query and retrieval capability is provided via SQL.

RDA is currently a GOSIP advanced requirement. In particular, an RDA application could specify the GOSIP FTAM as a choice for transfer of information. It is possible for RDA and other GOSIP products to be integrated in the future via the ACSE (see sec. 7). The SQL is a component of the APP.

10.2.4 FDDI

FDDI will be incorporated into GOSIP as a subnetwork technology. FDDI may also be used to support other protocols and applications. The NIST and other organizations have active FDDI research programs. Users should expect several new applications of FDDI to appear over the next 5 years.

10.2.5 POSIX

POSIX (Portable Operating System Interface for Computer Environments), which is sponsored by the Technical Committee on Operating Systems (TCOS) of the IEEE (Institute of Electrical and Electronics Engineers (IEEE) Computer Society), is a set of standard interfaces to an operating system, which allows applications to be ported among various heterogeneous POSIX operating POSIX is the first attempt to specify a standard set of program calls and command line interfaces for an operating system. In the future, many operating systems are expected to offer compliant interfaces and subroutine libraries. A revised POSIX FIPS has been issued in September 1990 as FIPS 151-1.

The GOSIP FIPS and POSIX FIPS are complementary, and their effect is expected to be synergistic. The GOSIP standard will be used to achieve interoperable data communications between computer systems. The POSIX standard will be used to provide a favorable software development environment for many applications, including OSI protocols. Furthermore, POSIX will permit portability of applications software. Federal agencies should ensure in procurements that GOSIP and POSIX requirements are properly integrated.

IEEE working groups are developing the following standard network interfaces: (1) a process-to-process (through a network) interface which will include standard interfaces to the OSI Session and/or Transport layers, (2) a standard set of interfaces for remote procedure call (RPC), (3) a standard set of interfaces for Transparent File Access (like NFS), (4) a standard set of directory services interfaces (including OSI X.500). (5) a standard set of X.400 interfaces, and (6) a standard set of interfaces to FTAM and MMS. Other working groups may be added in the future as needed.

10.2.6 Security

The initial GOSIP security specification is limited to a security option for the Connectionless Network Protocol. Work is now underway at the NIST and the National Security Agency (NSA) to develop a set of security protocols for use with GOSIP. An outline of the security requirements for GOSIP is given in an appendix to the Version 2 GOSIP FIPS. An initial set of security protocols is planned for the Data Link, Transport and Network Layers, as well as for the electronic mail application. A key management protocol will also be required.

10.2.7 CALS

Computer-aided Acquisition and Logistic Support (CALS) is a joint DOD/Industry strategy for the transition to highly integrated and near-paperless processes for engineering, manufacturing, and product support. Recently released DOD directives give preference to digital delivery of technical information on major systems contracts. Technical solutions to common data delivery, interchange, and access requirements are based on a family of standards already developed by CALS participants. The increased integration of processes will occur in an industrial environment of shared, distributed databases and electronic commerce in the 1990s and beyond. A framework of standards to support such integration is being defined.

Many CALS implementations will use GOSIP communications protocols to establish the improvement of functional processes and electronic commerce needed. Products supporting CALS are emerging, and will increasingly be able to take advantage of GOSIP functionality.

Close cooperation is maintained between CALS and GOSIP, and many complimentary projects are underway. NIST is activly supporting DOD in the CALS development, and intends that the GOSIP and CALS efforts are consistent and complementary.

10.2.8 Future Formats

Future versions of GOSIP will include information on how to identify and transport exchange formats such as Computer Graphics Metafile (CGM) and Standard Generalized Markup Language (SGML). These are described briefly below.

CGM specifications ensure a common file format for graphical data. The CGM standard permits transmission and storage of graphics information between different graphical software systems or different graphical devices. This graphical information may be stored in a device-independent manner.

SGML standardizes the application of the generic coding and generalized markup concepts. It provides a coherent and unambiguous syntax for describing whatever a user chooses to identify within a document. It is a metalanguage for describing the logical and content structure of a document in a machine-processable syntax.

An Application Profile (AP) defines additional requirements beyond FIPS SGML to ensure interoperability of implementations. MIL-M-28001 is an Application Profile for technical military publications. The plan is to develop an SGML Document Application Profile (SDAP) be extending MIL-M-28001 to be more useful to generic documents. Once the extensions are completed, SGML will be included as a GOSIP interchange format

10.3 General Advice

In practice the various standards development groups will have resolved major technical questions in creating the particular processing standard, but agencies may still have concerns about internal application of these standards. Agencies may also have concerns about supplemental or optional OSI services required to properly integrate GOSIP with other work (in particular, other components of the APP).

Federal agencies should:

(1) consult NIST to determine what Federal Information Processing Standards are available and what new technology will be included in GOSIP in the future (by consulting the Appendices in the GOSIP FIPS),

(2) in a long-term OSI acquisition strategy and procurement process, continually monitor the status of emerging Federal standard-setting efforts and include this new work in future procurements, and

(3) designate certain officials to consult with vendors when considering a solicitation to determine any conflicts between an agency's communication requirements and other computer-related requirements, as well as to resolve these conflicts if they arise.

APPENDIX A

OSI TUTORIAL INFORMATION

This appendix gives tutorial and explanatory information on the protocols referenced in the GOSIP Version 2 FIPS. This technical material is presented as an aid to understanding content of sections of the Users' Guide.

This appendix is organized as five sections. The first portion deals with network technologies; the second portion describes the Transport Layer. The third portion describes the FTAM (File Transfer, Access and Management) protocol, the next portion describes the MHS (Message Handling Systems) protocol, and the final portion describes the Virtual Terminal (VT) protocol.

A.1 Network Technologies Tutorial

This section provides tutorial information on network technologies that are referenced in GOSIP. The first subsection gives a general introduction. Successive subsections describe specialized network designs. For additional material on these topics, please consult appropriate references, given in Appendix B.

A.1.1 Introduction

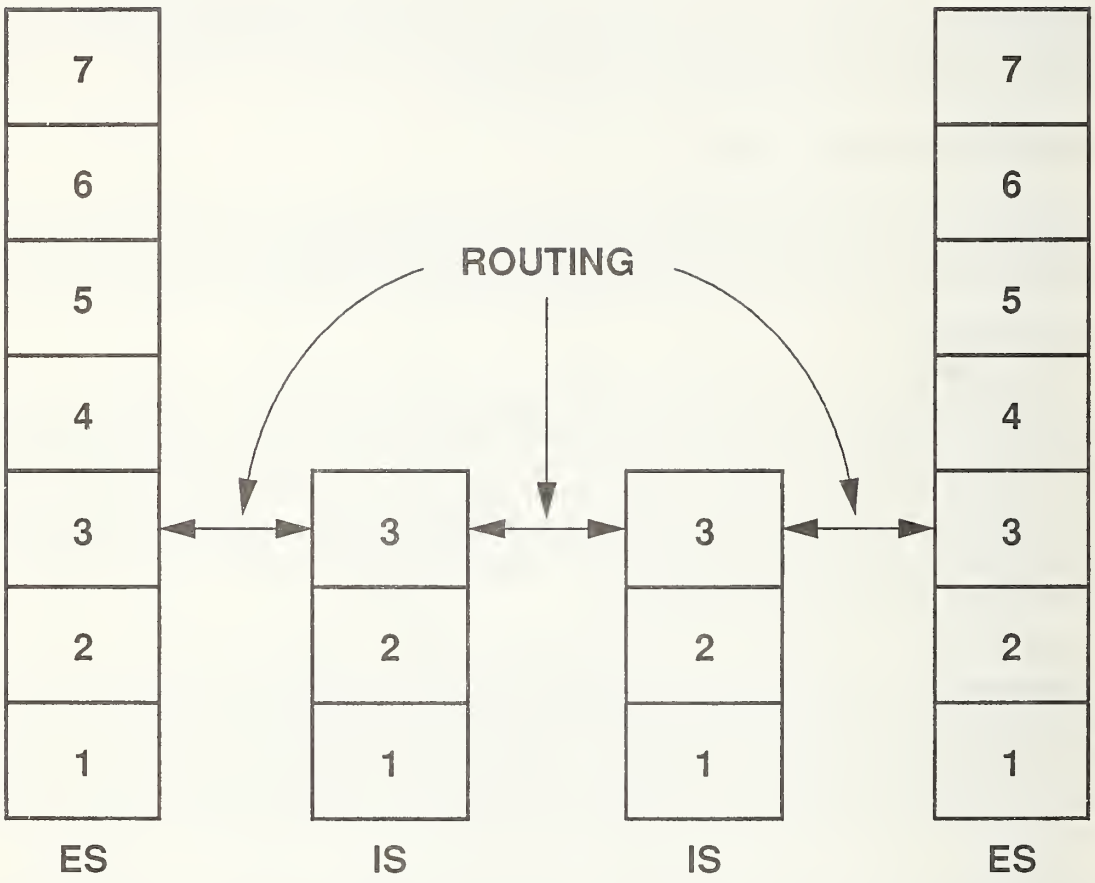
A GOSIP network can be composed of different subnetworks which may use different technologies to move data. These subnetworks are connected by intermediate systems which relay messages between different subnetworks and mask the differences in the various technologies. There are six technologies specified in GOSIP as follows: ISO 8802/3 (CSMA/CD), ISO 8802/4 (token bus), ISO 8802/5 (token ring), X.25 wide area network, point-to-point links, and ISDN. CSMA/CD stands for "carrier sense multiple access with collision detection." The ISO 8802/3, 8802/4, and 8802/5 standards are identical to the respective IEEE 802.3, IEEE 802.4, and IEEE 802.5 standards.

GOSIP applies to both intermediate systems and end systems. Intermediate systems are relay systems that interconnect two or more subnetworks. GOSIP protocols from at least Layers 1 through 3 are contained in intermediate systems. End systems, on the other hand, are terminus systems which originate or receive Transport messages (user-oriented message flows). GOSIP protocols included in end systems are those from OSI layers 1 through 7. Intermediate systems perform routing and relaying of packets between end systems to support the Network Layer service provided in those end systems. Figure 22 illustrates these concepts.

A concern for users is to ensure that data has been transferred correctly between end systems, possibly passing through different types of subnetworks, not all of which are equally reliable. This subsection discusses the different technologies incorporated in layers 1-3 (Physical, Data Link, Network) of the OSI Reference Model. Architecturally, ISDN is layered in the same fashion as the OSI Reference Model, although many ISDN protocols describe different functionality than that described by the OSI protocols belonging to the same layer.

As Figure 23 shows, the GOSIP subnetwork technologies may be architecturally divided into local area networks and wide area networks. Standards development emphasizes certain features of the technologies under consideration, depending on their application. For instance, local area networks have hosts separated by short distances, and wide area networks have hosts separated by longer distances. These local area networks and wide area networks are integrated using the CLNP (Connectionless Network Protocol).

Partitioning of the OSI Physical Layer, Data Link Layer, and Network Layer functionality differs between local area networks and wide area networks, but all of the functional elements of each layer must be included in each technology. Below, layers 1-3 are described in terms of OSI layer functionality. Subsections A.1.2 and A.1.3 describe how the local area network and wide area network standards map into the OSI Model as shown in the columns of Figure 23.



ES = END SYSTEM
IS = INTERMEDIATE SYSTEM

FIGURE 22
GOSIP ROUTING SUMMARY

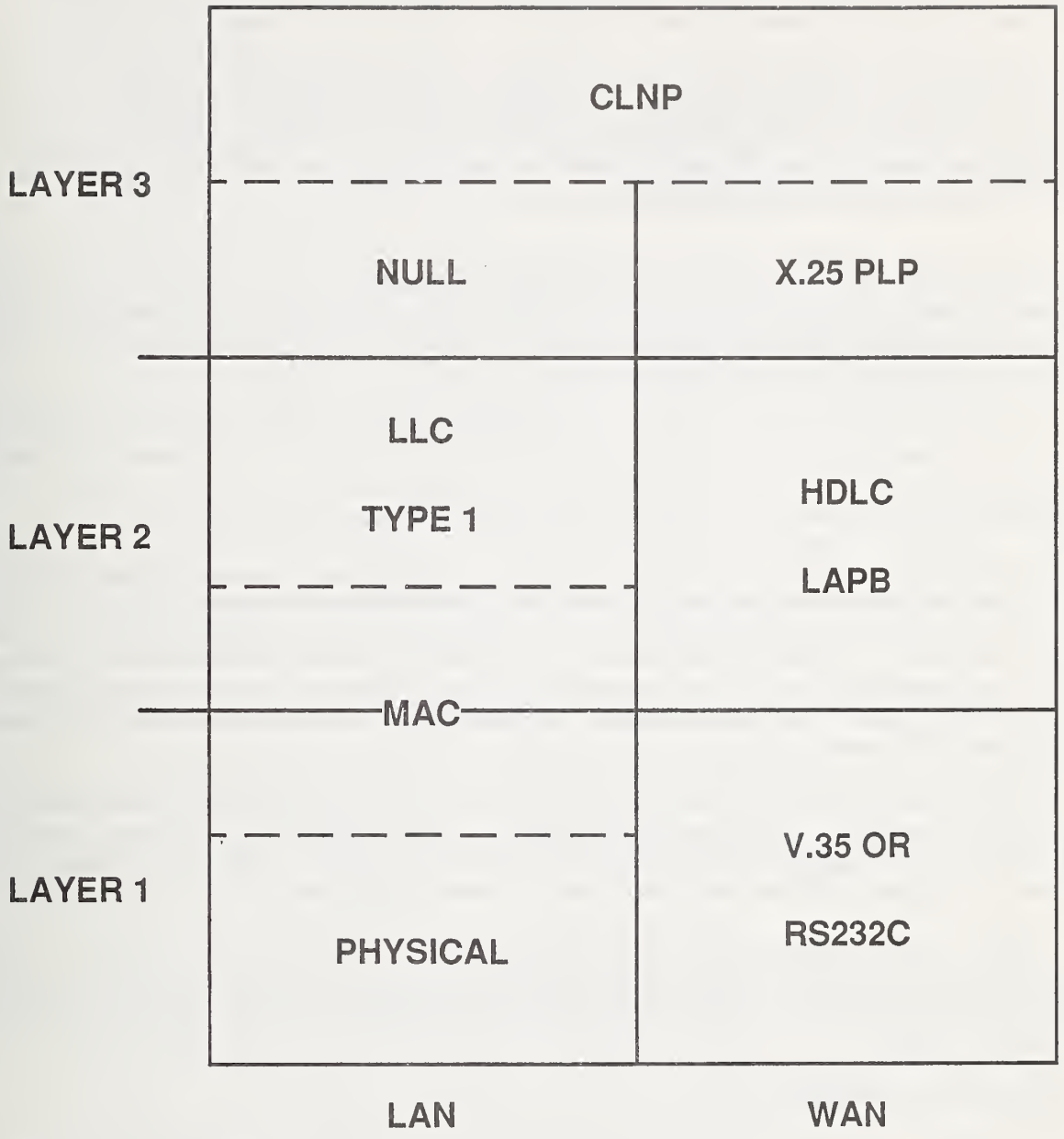


FIGURE 23
GOSIP SUBNETWORKS

The Physical Layer is capable of transmitting bits over a communication channel. The Physical Layer defines the conventions for transmitting and recognizing bits as either 0 or 1. Some concerns of the Physical Layer are how many volts should be used to represent a 1 and how many for a 0. how many microseconds make a bit, whether transmission may proceed simultaneously in both directions, how many pins the network connector has and what the use of each pin is. The types of cable technology used include coaxial cable, twisted-pair, and fiber optics. The Physical Layer provides modulation techniques sufficient to represent a signal across an imperfect cable. It should be noted that the Physical Layer does not guarantee error-free transmission of bits; this is left to higher layers.

The task of the Data Link Layer is to take the raw transmission facility provided by the Physical Layer and transform it into a link that appears substantially free of transmission errors to the Network Layer. It performs this function by taking bits, forming them into data frames and transmitting the frames sequentially. The Data Link Layer provides error detection and correction capability (involving two computers directly connected) across a line between nodes of a subnetwork.

The Data Link Layer checks the number and position of bits received, and performs various calculations to determine if there is an error, e.g., if a "1" bit is accidentally received as a "0". Synchronization of sender and receiver is important in this layer. Both the Physical and Data Link Layers apply only to "box-to-box" communications; that is, management of bits between directly-connected computers.

The Network Layer performs the routing and relaying of data between hosts on the same or different subnetworks. The Network Layer assures that data packets are correctly routed toward the destination. The network header is examined by Network Layer entities to determine where to send the packet next. Along the way packets may be fragmented. Since different packets and fragments may take routes through different sequences of subnetworks, the packets and fragments may arrive out of order and must be reassembled (placed together) at the destination. Although reassembly is a layer 3 function, reordering is a layer 4 (Transport) function which will be mentioned later.

The CLNP assumes a datagram level of service from the subnetworks (either local area networks or wide area networks). Datagram service implies that data packets are sent as individual isolated units, which may arrive out of order, in fragments, more than once, or not at all. It is up to a higher layer of functionality (Transport) to ensure in-order, accurate delivery of data between end systems.

The ES-IS dynamic routing protocol (ISO 9542) may be used in conjunction with the CLNP over local area networks, and may also be used over HDLC LAP B for point-to-point links. In an ISDN, service is provided to the Connectionless Network Protocol (IS 8473). The Connection-Oriented Network service may also be used with ISDN.

A.1.2 Local Area Networks

Three different local area network technologies are discussed below. These incorporate the functionality of the lowest three layers of the OSI Reference Model. There are many different kinds of local area networks; three types have been selected for inclusion in GOSIP because they are generic in applicability, are relatively simple to implement, provide acceptable performance in most instances, and are, in general, widely available.

Local area networks have three distinctive characteristics: (1) a diameter of not more than a few kilometers, (2) a transfer rate exceeding 1 Mbps (megabit per second), and (3) ownership by a single organization. Since distances are short, it is economical to install high-bandwidth cable between hosts. These cables may be divided into channels, where each channel defines a different path of communication.

The GOSIP link layer is composed of the logical link control (LLC) Type 1 sublayer and media access control (MAC) sublayer. The MAC sublayer manages the Physical Layer and mediates access to it by means of an access discipline, e.g., CSMA/CD. The LLC Type 1 sublayer provides a mapping between the LLC Type 1 (datagram) services and the MAC services.

Frame delivery is provided at locations called LSAPs (link service access points) for local area networks. Datagram service implies the passing of data packets as isolated units, where packets may arrive out of order, more than once, or not at all.

As shown in figure 23, the Physical Layer is bundled with the MAC, and the LLC Type 1 provides datagram service to the CLNP above it. The MAC provides a cyclic redundancy code. The Physical Layer-MAC combinations are different for each local area network technology chosen. The interfaces between the physical medium, the MAC, and the LLC are distinct, but do not always correspond evenly with the functional layer interfaces defined in the OSI Reference Model. This does not matter, because the LLC maps nicely to the Data Link service boundary.

Local area networks are distinguished by the access method. Access to this cable may be: (1) deterministic, or (2) random. In deterministic access, there is a predefined scheme by which a host is guaranteed access to a cable. In random access, open competition for the use of the cable occurs, involving any hosts who wish to transmit. The three kinds of local area networks described below include both types of access, and offer advantages or disadvantages depending upon a user's particular requirements and existing configurations.

CSMA/CD is an example of random access networks. Only one sender can transmit on the cable at one time. A host may attempt to send immediately if desired, without waiting for a predefined signal. Because of a very small propagation delay for a signal on a line, any host connected to the line can "listen" to the line before attempting to use it. If two hosts attempt to use the line at the same time, a collision occurs, and both hosts immediately stop transmitting. Each host tries again later, using a "backoff" algorithm. The retry times computed are likely to be different for each host.

A well-known implementation of this scheme, the IEEE 802.3 standard, is the basis of the GOSIP-compliant CSMA/CD. There are several minor differences between Ethernet, a precursor, and IEEE 802.3. These differences are in the way the backoff time is calculated, and in one of the link-layer header fields. As mentioned previously, the IEEE 802.3 standard is identical with the IS 8802/3 standard referenced by GOSIP. The IS 8802/3 standard includes both baseband and broadband coaxial cable in the specification.

The principal advantages of CSMA/CD are low cost, simplicity, wide availability, and quick response time in light to moderate traffic loads (below 40 percent). The principal disadvantage is a marked degradation in performance under heavy traffic conditions.

The token bus scheme (IS 8802/4) uses a bus (single cable) architecture like that used by CSMA/CD, with stations connected to the cable. Unlike CSMA/CD, however, the token bus scheme uses a token passed from host to host to regulate access to the cable. An algorithm controls the logical ordering of hosts set to receive the token; this order may or may not be the physical order of hosts on the cable. A host may only send data when it has the token; after finishing the host relinquishes the token to the next host in the logical ordering. Thus, there is no contention for the cable as in CSMA/CD. Token bus schemes typically use broadband transmission on a coaxial cable.

The advantage of the token bus scheme is that it provides regulated access and deterministic performance even under heavy load (to at least 80 percent). The disadvantage is the complexity of the implementation, particularly that of the algorithm used to control host ordering, as well as the resultant high cost. Still, by applying a token bus technology a user is able to derive better performance in a variety of situations than with CSMA/CD. GOSIP adopts the token bus scheme in the IS 8802/4 standard.

The organization of token ring networks is fundamentally different from a CSMA/CD network. In contrast to a carrier sense network which is basically a passive, electrically connected cable onto which all stations tap, a ring network is actually a series of point-to-point cables between consecutive stations. The ordering of activity in a ring network is by the physical order of the stations. The IS 8802/5 technology allows operation on twisted pair and coaxial cable. A host must have the token in order to transmit, and the token ordinarily moves around the ring in round-robin fashion. Timers are used to control token holding

time; when a timer expires, the host must relinquish the token.

The advantage of this scheme is that good performance is obtained, even at moderate-to-heavy traffic loads because access to the ring is regulated. Disadvantages are the need for token maintenance and delay in sending even in light traffic conditions. However, for GOSIP users, the token ring approach offers a viable alternative to the other technologies in effectively transferring data between hosts. The GOSIP token ring technology is based upon the IS 8802/5 standard.

A.1.3 ISDN

The central idea behind ISDN is that of the digital bit pipe, a conceptual pipe connecting the customer and the carrier through which bits flow in both directions. The digital bit pipe supports multiple independent channels by time division multiplexing of the bit stream. Two principal standards for the bit pipe have been developed: a lower bandwidth standard for home use, and a higher bandwidth standard for business use. A network terminating device, NT1, is placed by the carrier on the customer's site. For business use, a separate device, NT2 (a PBX (private branch exchange)), is connected to NT1; NT2 provides a real interface for telephones, terminals, and other equipment.

An ISDN PBX can interface directly to ISDN terminals and telephones. For non-ISDN devices, terminal adapters can be installed to handle the conversions required.

CCITT has defined four reference points (R, S, T and U) between various devices. The U reference point is the link between the ISDN exchange in the carrier's office and NT1. The T reference point is the link between the connector on NT1 and the customer. The S reference point is the interface (boundary) between the ISDN PBX and the ISDN terminals. The R reference point is the link between the terminal adapter and non-ISDN terminals.

CCITT defines "interface" for ISDN as being the boundary between the carrier's equipment and the customer's equipment. Six channel types (A,B,C,D,E,H) have been standardized. Two of interest to GOSIP are the B Channel (64 kbps digital channel for voice or data), and the D Channel (16 or 64 kbps digital channel for out-of-band signaling). Three combinations of channels on the digital bit pipe are: (1) basic rate (2B + 1D), (2) primary rate ((23B + 1D) in US), and hybrid (1A + 1C). The interfaces corresonding to (1) and (2) above are the basic rate interface (BRI) and the primary rate interface (PRI). These can be used to support either circuit switching or packet switching, depending on the nature of the traffic.

Layer 1 of the CCITT ISDN standard describes the physical interface from customer premises equipment to a public network. Layer 2 provides a D Channel link layer protocol to guarantee end-to-end error correction and retransmission. Layer 3 of the CCITT ISDN standard provides D Channel signaling protocols that are used to establish and route transmissions.

Internationally there are two areas of ISDN incompatibilities. The first incompatibility occurs because carriers and central office switch makers in different countries are working with various standards for connecting customer premises to the public network. These differences have arisen because of the range of options in CCITT ISDN standards. The other major incompatibility is that carriers are not yet equipped to handle international ISDN D Channel transmissions. It is expected that these problems will be resolved in the future.

A trial was conducted involving OSI applications communicating using ISDN subnetwork capability; documentation [NIST 7] is available. The following ISDN functions were demonstrated: CLNP over ISDN X.25, optional CONS over ISDN X.25, X.25 D Channel, X.25 preallocated B Channel, BRI (Basic Rate Interface), and S and T reference points. The utility in combining OSI and ISDN in the manner described was demonstrated.

A.1.4 X.25 Wide Area Networks

The X.25 protocol is connection-oriented. The source and destination addresses only have to be given at the beginning of a connection. X.25 is used by GOSIP as a subnetwork for long-haul transmission.

For X.25, the Physical Layer specification for GOSIP is typically RS-232-C for line speeds up to 19.2 kilobits per second, and CCITT V.35 for line speeds above 19.2 kilobits per second. The Link Layer of X.25, LAPB (link access protocol-balanced), is responsible for correct transmission of packets between the end system and the DCE (i.e., data circuit-terminating equipment or X.25 packet-switching node). Here packet switching implies the proper routing and relaying of data packets. The LAPB has the following features: (1) it implements a checksum to ensure that end system/X.25 node frame transfers are received correctly, (2) the flow of frames between the end system and node is controlled by a window mechanism, and (3) frames received are acknowledged and incorrectly received frames are retransmitted.

The X.25 Packet Layer Protocol (PLP) operates over LAPB and provides the X.25 virtual circuit (VC) interface. VCs are logical connections between DTE (data terminal equipment) nodes. Since the CLNP assumes a simple datagram interface to its underlying subnetworks, a collection of functions is defined to map between the service assumed (datagram) and the service provided (VC). These subnetwork-dependent convergence functions open X.25 VCs to destinations identified by the subnetwork address passed down from the CLNP with each datagram request, accept VCs from remote systems, pass to CLNP messages received on X.25 VCs, and close VCs when there is inactivity. The subnetwork dependent convergence function thus isolates the CLNP from the specific characteristics of the underlying subnetwork (in this case, that it is connection-oriented).

In general, the boundaries between the Physical Layer, the LAPB, and the X.25 PLP are quite distinct. These boundaries correspond well with layer boundaries defined in the OSI Reference Model.

The CCITT X.25 standards have evolved from the 1980 X.25 Recommendation to the 1984 X.25 Recommendation, and the evolution continues to the 1988 X.25 standard. Version 2 of GOSIP references the 1984 X.25 Recommendation. The main difference between 1980-based and later X.25 Recommendations is that later X.25s include all capabilities necessary to establish and maintain connection-oriented network service between users whereas 1980 X.25 requires a special protocol called the SNDCP (subnetwork dependent convergence protocol) to achieve this same level of service. Guidance for moving from 1980 X.25 to 1984 X.25 is given in section 7.

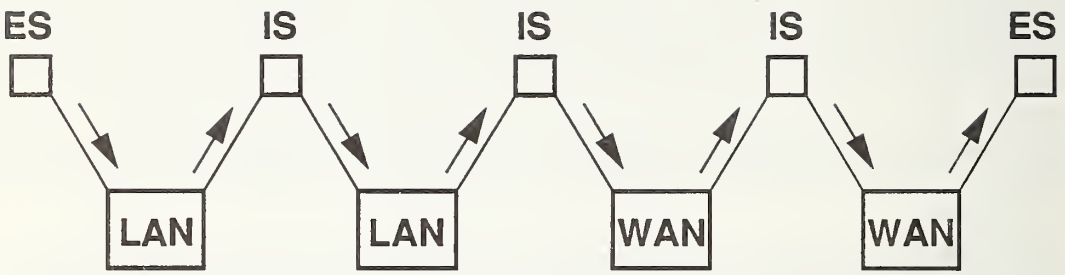
A.1.5 CLNP (Connectionless Network Protocol)

GOSIP subnetworks may be of different types as described above with different specifications, and for expanded interoperability it is necessary to interconnect them so that an end system on one subnetwork can communicate with an end system on a different subnetwork. The means used in GOSIP to interconnect subnetworks is the CLNP; this protocol provides OSI Network Layer routing between interconnected subnetworks, in order to move a data packet from source to destination. The CLNP [ISO 16] provides a datagram service to the Transport Layer above, and a datagram service is provided to the CLNP from either a local or wide area network.

The CLNP includes provisions for segmenting data packets for greater efficiency. A "lifetime" feature indicates the maximum time a data packet may exist in the network before being dropped, and the reassembly timer gives a time deadline for recreation of complete data packets at the destination end system. Each protocol data unit header contains a destination address, which is used by intermediate systems to route the packet to the correct destination end system. Some other fields in the header are: security, priority, and segment number. The CLNP is typically used to link together different local area networks to create a single larger internetwork, and may be used to link together different wide area networks as well (or to link together a mixture of local area and wide area networks). Figure 24 illustrates this.

A.1.6 ES-IS Routing Protocol

Simple routing protocols provide the capability for hosts (end systems) and routers (intermediate sys-



ES = END SYSTEM
IS = INTERMEDIATE SYSTEM
LAN = LOCAL AREA NETWORK
WAN = WIDE AREA NETWORK

FIGURE 24
CLNP FUNCTION

tems) to locate one another. This eliminates the need for static configuration information and permits hosts to be moved without reconfiguration. The ES-IS protocol provides hosts with an entry point into a system of routers.

The end system (ES) to intermediate system (IS) protocol uses adaptive routing to support the movement of data packets between an intermediate system and destination end systems on the same subnetwork (see sec. 8). This routing is dynamic; that is, the path will change depending on such factors as congestion, topology, and the network traffic. This routing is done based on the source address and destination address encountered in the data packet header. The ES-IS protocols provide robustness, correctness, simplicity, fairness, stability, and optimality.

A.2 Transport Layer Tutorial

The Transport Layer of the OSI Reference Model provides reliable end-system-to-end-system data transfer. There are five classes of Transport service; these are known as Class 0 through Class 4. Some Transport classes (including Class 4) provide retransmission of lost data, flow control, and reordering of data packets. Transport Class 4, which provides the highest level of capability of the five classes defined, is required for GOSIP systems. Transport Class 0 has the lowest level of functionality of the five classes. There is an increase in functionality with an increase in class number for Transport Classes 0, 2, and 4. Classes 1 and 3 have, in general, not been widely accepted or implemented. The reason that Transport Class 4 was selected for GOSIP is that its use promotes the maximum degree of interoperability between different systems, and that it is required for operation over the CLNP.

Transport interfaces may be exposed or embedded. An exposed interface may support non-standard applications. Conventions must support the requirements of IS 8073, the Transport Service Definition. Acquisition authorities must consider several factors in determining the type of interface required, including the number and kind of users of the Transport service.

The Connectionless Transport Protocol (CLTP) is used to support the Connectionless Transport Service (CLTS); the CLTP is to be used only as an option among participants with a similar capability. The CLTP is included in GOSIP Version 2 so that non-OSI applications (for example, the Network File System) can take advantage of its services. The CLTP may only be specified as an addition to the Connection-Oriented Transport Protocol.

A.3 File Transfer, Access and Management (FTAM) Tutorial

This section gives a general description of the services provided by FTAM and what additional capabilities are needed to make it work.

A.3.1 FTAM Protocol, Service, and Model

The File Transfer, Access and Management (FTAM) Standard [ISO 2-6] allows for the effective transmission, access operation, and management capabilities of a variety of different file types and formats across electronic media, without detailed knowledge of the particular charcteristics of the remote machines.

Briefly, FTAM allows different applications or different users of applications to transfer information without specific knowledge of the other system's characteristics. FTAM also allows users a greater degree of control over the file activity, as well as an expanded set of capabilities and features. Futhermore, all of this is accomplished in a completely automated fashion, and in a globally interconnected environment. Other applications may use FTAM as a supporting service. In fact, FTAM can be used locally as a set of callable library routines.

The FTAM standard is composed of five parts: a General Description, a Virtual Filestore, a File Service Definition, a File Protocol Specification, and a Protocol Implementation Conformance Statement (PICS). The General Description deals with basic terminology and broad FTAM concepts, and should be read first. The File Service Definition gives an overview of FTAM services provided to the user. The Virtual Filestore section gives information on the central model used by FTAM. The File Protocol Specification gives a detailed description of the protocol interactions necessary to accomplish the FTAM activity. The PICS gives information useful in FTAM testing.

In addition, there are two addenda as follows: overlapped access, and filestore management. Overlapped access deals with reading to and writing from different portions of a file simultaneously; filestore management involves an extensive set of directory commands, including search, list, and change directory.

Currently, the standard is an IS (International Standard) in the International Standards Organization. The addenda will progress to IS by 1990. Furthermore, the FTAM section in the NIST Workshop Agreements [NIST 1] is based upon the IS FTAM documents. All of the FTAM products marketed by vendors are expected to be based upon the FTAM IS.

The services of FTAM provided to the user are: (1) the ability to communicate about files without specific knowledge of the other system, (2) the facilities to express explicitly what the users require, (3) the ability to specify uniform file properties, (4) the ability to specify record-level file access and positional file transfer, and (5) detailed file management. This list is expected to grow over time as more special-purpose applications are written which may use FTAM as a supporting service.

Some examples of applications which may use FTAM are the following: distributed database management applications, document retrieval and updating (library information services), and specialized "messaging" systems composed of long text messages. Applications which transfer large amounts of structured data reliably end-to-end between heterogeneous systems, large accounting and payroll applications, large inventory control applications, and worldwide automated financial integration systems are also included.

FTAM is a two-party file transfer protocol; in other words, there is a controller of the file activity (initiator) that directs the action, and a responder, that responds to the initiator in a passive role. All file transfers and access operations occur between initiator and responder. Three-party file transfer is a subject of discussion for the future. An FTAM implementation may act as initiator, as responder, or as both.

FTAM is defined in terms of functional units and service classes. Service classes are described in terms of functional units; some of these are mandatory within a service class and some are optional. The functional units in FTAM are kernel, limited file management, enhanced file management, read, write,

grouping, recovery, and restart.

Service classes are: transfer, management, access, transfer and management, and unconstrained. The names indicate the functional capabilities. For functional units, the kernel is the basic set of FTAM capabilities. Limited file management deals with the ability to create, delete, and interrogate properties of files. Enhanced file management deals with the ability to change file properties. Grouping allows concatenations of FTAM requests for efficiency purposes.

There are file attributes and activity attributes. File attributes are globally unique and may be seen by anybody accessing the file. Activity attributes are particular to a connection and are only visible to the user of the connection. Via FTAM, a user may query the values of these attributes and possibly change these values. Table 3 gives a partial list of these attributes.

Table 3 - FTAM Attributes

FILE ATTRIBUTES

filename, permitted actions, contents type,
storage account, date and time of creation,
date and time of last modification, identity of creator,
identity of last modifier, file availability,
filesize, access control

ACTIVITY ATTRIBUTES

active contents type, current access request,
current initiator identity, current location,
current processing mode, current account,
current concurrency control

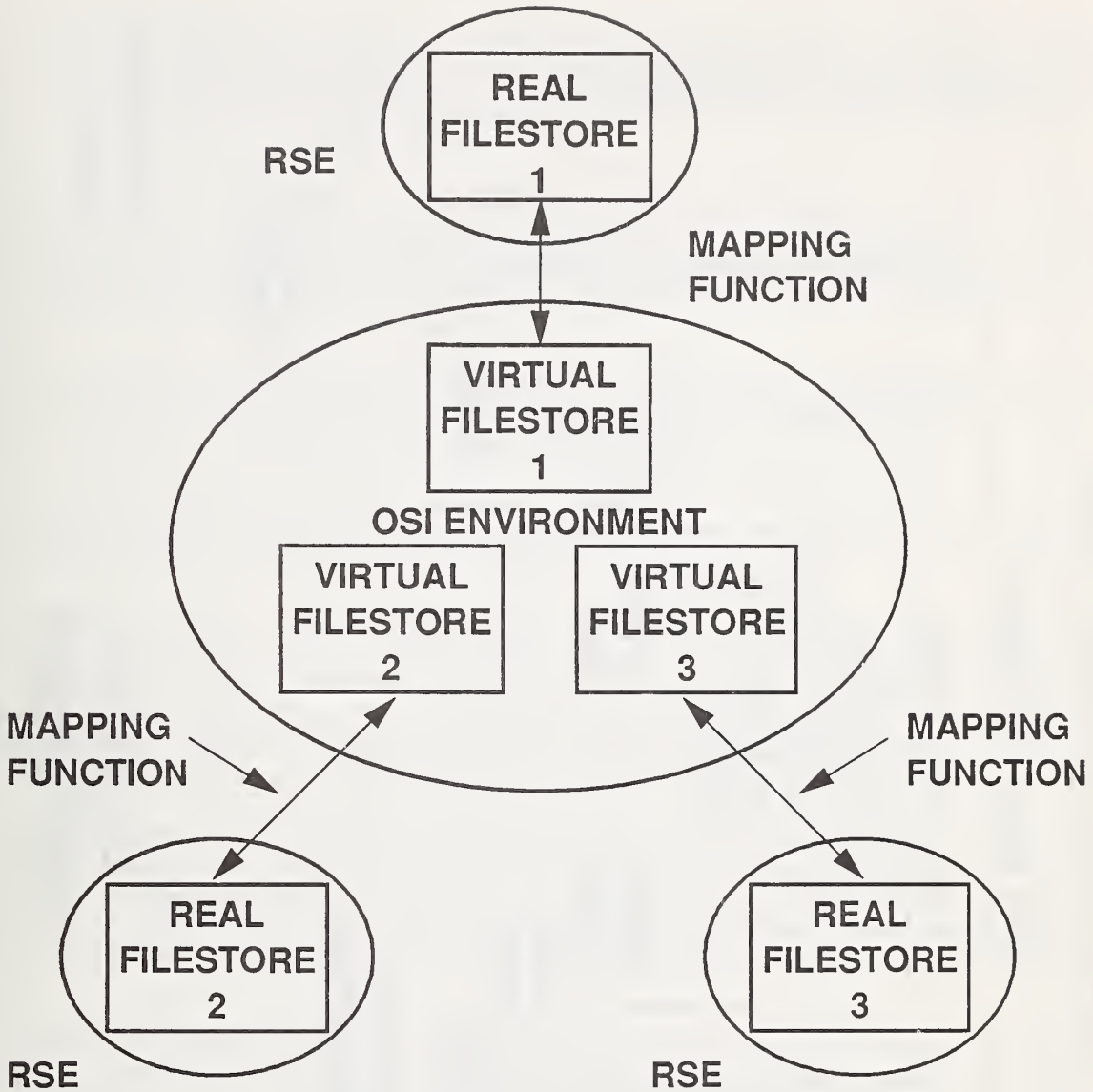
FTAM embodies the concept of a virtual filestore. In the OSI environment, there is one conceptual representation of this virtual filestore model. In the real environment, there are multiple real filestore implementations. Thus there must be mapping between a real filestore and a virtual filestore. The nature of this mapping is a local issue. Figure 25 illustrates this mapping.

The generic FTAM model is applicable to most FTAM systems in use today. All of the characteristics of the virtual filestore can be recognized and interpreted by any OSI file system, so the essence of communication is through this model. As the need for other models occurs in FTAM, they will be developed.

The FTAM service may be described as a series of regimes. Regimes may be defined as environments which may be entered and exited via confirmed services. The first or outermost regime is the application association regime; this involves setting up an FTAM activity within the context of an association. Service primitives involved in this effort are F-INITIALIZE to set up, and F-TERMINATE or F-ABORT to exit. Figure 26 depicts the FTAM regimes.

Once the first regime is entered then filestore management is invoked. This is where file directory services will be available in the near future. Next comes the selection/creation regime. This is the regime where the attributes of a file are specified, for a file already existing on a destination system (F-SELECT), or new attributes of a file are created (F-CREATE). The corresponding service primitives which terminate this regime are F-DESELECT and F-DELETE, respectively. This regime involves specifying the properties of a file.

Once the file selection regime is entered, attributes can be queried or changed. The F-READ-ATTRIB



RSE = REAL SYSTEMS ENVIRONMENT

FIGURE 25
MAPPING BETWEEN REAL SYSTEMS AND OPEN SYSTEMS

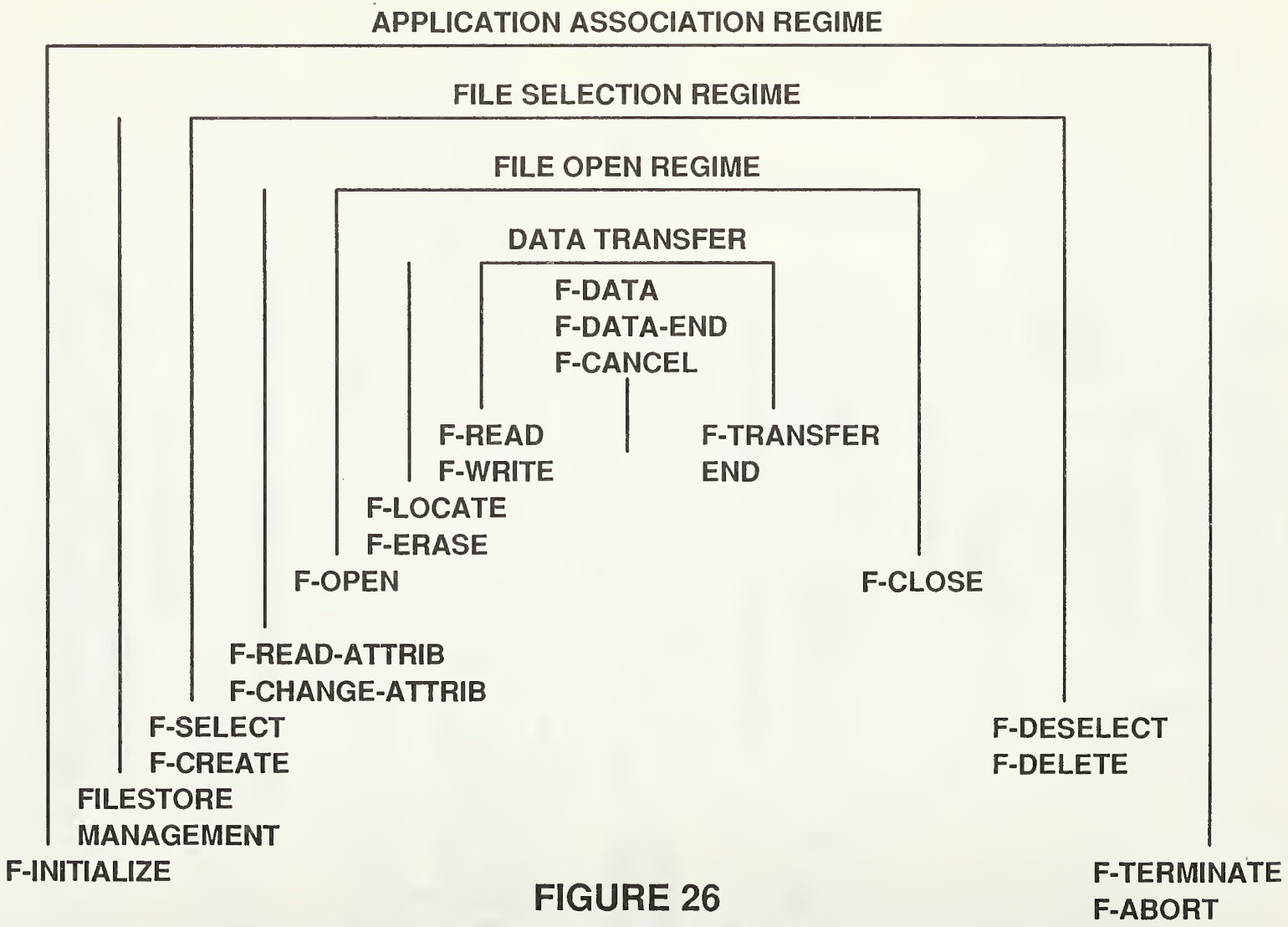


FIGURE 26
FTAM REGIMES

service primitive is used to query attributes. The F-CHANGE-ATTRIB service primitive is used to change attributes.

Next comes the regime where the file is opened; this implies that the file contents may be accessed by the initiator. The service primitive to invoke here is the F-OPEN service primitive. This primitive has a number of important parameters. In the open regime are contained the locate and erase actions. These actions are represented by the LOCATE and ERASE service primitives. The LOCATE action finds a specified record in a file, and the ERASE action removes a specified record.

The next actions to invoke are those of F-READ and F-WRITE; F-READ is used to read the file, and F-WRITE is used to write the file. These actions generally occur in opposite directions. Among the primitives accessed are F-DATA, as well as F-DATA-END and F-CANCEL. F-DATA actually carries the data, F-DATA-END terminates the data, and F-CANCEL cancels the action. The entire data transfer action is completed by an F-TRANSFER service primitive.

F-CLOSE terminates the OPEN regime and makes access to the file contents impossible. The service primitives to abruptly exit from an FTAM activity are F-U-ABORT and F-P-ABORT. F-U-ABORT is issued by either file service user; F-P-ABORT is issued by the service provider.

As mentioned previously, the FTAM model is a two-party model. There is an initiating file service user, who is separated from the FTAM Initiator by a user interface. The FTAM Responder is also connected to a responding file service user by a user interface. Figure 27 illustrates this scenario.

A virtual filestore schema is composed of a: (1) file, which contains file attributes and file contents, (2) filestore, which may contain a number of files, and (3) a connection, which involves active attributes and current attributes. These is a user attached to the connection. The schema is hierarchical with a (tree-like) structure. Specific parts of a file are defined using node identifiers, or File Access Data Unit (FADU) IDs. Many different access structures are possible. For example, one user may wish to view a file as essentially a flat structure, whereas another user may wish to view the file as having a hierarchical structure.

The properties of a virtual filestore are: (1) that it may contain an arbitrary number of files, (2) that the properties of each file are determined by global file attributes, (3) each file is either empty or has some contents and a structure, and (4) at most one file in the virtual filestore is bound to a particular FTAM regime at any one time. Also, a set of activity attributes is associated with each FTAM regime; these are particular to an FTAM activity. An arbitrary number of FTAM initiators may have FTAM regimes at any one time.

FTAM has a rich set of diagnostics, which convey detailed information about the status of an FTAM request. There is provision for users to include additional explanatory material where appropriate. FTAM has four classes of errors, from minor errors to errors which destroy the FTAM activity. Each of these classes is dealt with in an appropriate manner.

FTAM information is conveyed via special messages called service primitives. Each primitive describes a particular action taken by a file service user. These primitives include associated parameters, which are special fields containing common values. Each value has a predefined meaning. The sequence is as follows: first a request is made by one machine. This request is received by the destination machine, which sends back a response (either yes or no) to the request. This response is received by the requester as a "confirm" action.

Each of the service primitives has a list of parameters. These may be mandatory, optional or conditional. For example, for F-INITIALIZE, some parameters are: result, called application title, calling application title, responding application title, presentation context management, service class, functional units, attribute groups, files quality of service, and initiator identity. The parameters have particular values, and the ordering of parameters is important.

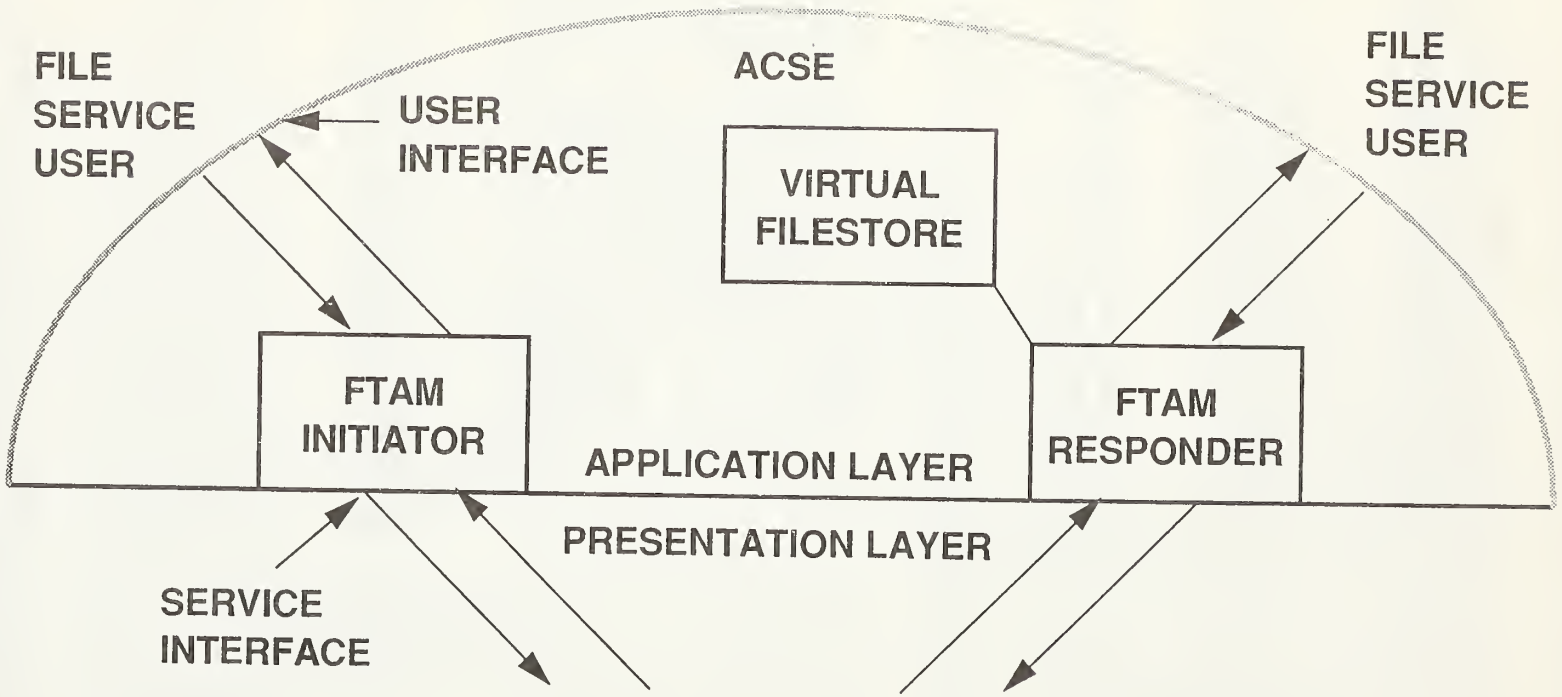


FIGURE 27
FTAM MODEL
(TWO PARTY)

The file access structure of FTAM is described hierarchically. There are various levels to this hierarchy; at each level are nodes, each of which may be connected to zero or one data unit. These nodes could be considered place-holders in a file, and represent locations. A corresponding concept is block or record position in a real file. There is a root node at level 0. The tree organization is hierarchical. A data unit corresponds to a block or record of data in a real file. There is a file access data unit (FADU) at each node, and FADUs encompassing multiple nodes. These FADUs represent (smaller or larger) portions of the file. Level numbers increase from the root downward; nodes at a fixed level may be siblings, and each node at a fixed level has zero, one or more children at a deeper level (higher level number). Figure 28 illustrates these concepts.

Access control is invoked in many different ways in FTAM. To start, the FTAM user has a set of permitted actions allowed for that user for that activity. Correspondingly, each file has a set of allowable actions attached to it. The FTAM user can only operate at the intersection of these capabilities. The requested access FTAM parameters specify the actions potentially allowable to the FTAM user.

File attributes describe generic properties of a file, and activity attributes describe generically the state or condition of an FTAM connection. In terms of FTAM file attributes and activity attributes, some common file attributes are: filename, permitted actions, contents type, storage account, date and time of creation, identity of creator, filesize, and future filesize. Other file attributes are access control, file availability, and legal qualifications. Some of the common activity attributes are active contents type, current location, current account, current access passwords, and current processing mode.

File types supported in FTAM are: sequential text, indexed sequential, sequential binary, directory, and random-access. Data types supported are: different versions of text (character sets), real (floating-point), integer, and boolean.

There are four types of FTAM information conveyed: FTAM data units, FTAM protocol information, FTAM structuring information, and abstract syntax information. An abstract syntax is the general description of the kinds of information that FTAM uses. It is necessary to convey the structure of an FTAM file before transmitting it between initiator and responder. The means by which FTAM conveys this information is document types and constraint sets.

Document types are specific descriptions of file structure; constraint sets are more general descriptions. For example, for an ASCII sequential text file with 80-character records delimited by CR-LF pairs, a document type name could adequately describe this. However, to describe all text files with sequential record structure, a constraint set name should be used. There are document types defined within the FTAM standard, and document types defined by the workshop. Each document type describes a specific file structure; this information is passed at F-OPEN time. Detailed descriptions of document types defined by the NIST/OSI Workshop are given in the NIST Workshop Agreements.

There is a one-time negotiation between initiator and responder when making any FTAM request. An initiator proposes, and a responder modifies the initiator's request by subsetting it, if necessary. Based upon the nature and characteristics of the request, the responder may accept or reject the request.

Several ISO contraint sets are allowed. Among them are: unconstrained (applies to entire file as atomic unit), sequential flat (simple sequential), ordered flat (indexed sequential), ordered hierarchical (hierarchically organized files with constraints), general hierarchical, and none The list of ISO document types is divided into: FTAM-1 (unstructured text file), FTAM-2 (sequential text file), FTAM-3 (unstructured binary file), FTAM-4 (sequential binary file), and FTAM-5. Table 4 summarizes these prominent document types.

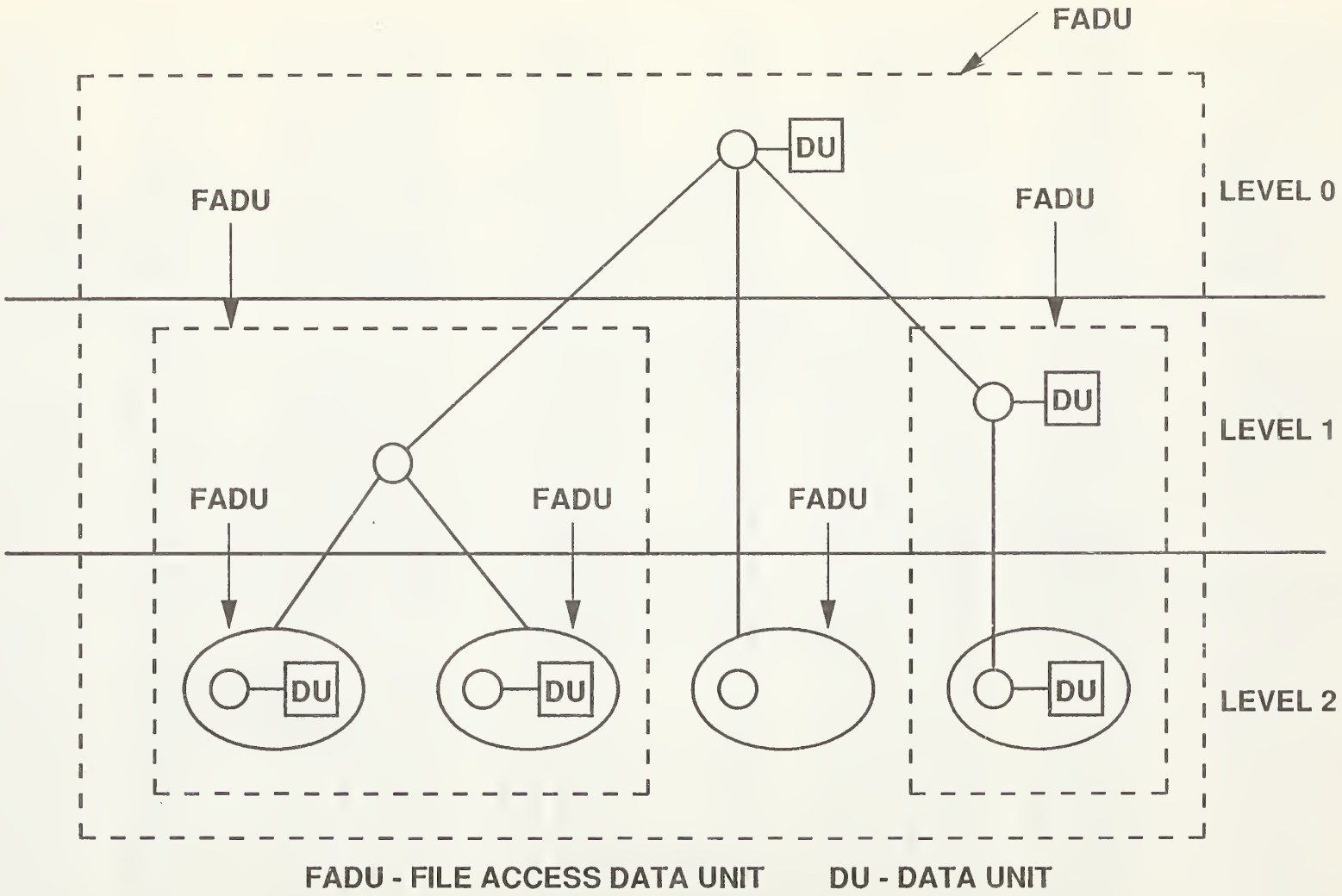


FIGURE 28
FILE ACCESS STRUCTURE

Table 4 - FTAM Document Types

NAME = FTAM-1

DESCRIPTION: unstructured text (a single character string with no delimiters)

==========

NAME = FTAM-2

DESCRIPTION: sequential text (some character strings separated by delimiters in a sequence, and order is important)

==========

NAME = FTAM-3

DESCRIPTION: unstructured binary (a single binary string with no delimiters)

==========

NAME = FTAM-4

DESCRIPTION: sequential binary (some binary strings separated by delimiters in a sequence, and order is important)

==========

NAME = FTAM-5

DESCRIPTION: simple hierarchical (series of records or blocks organized in a tree-like structure) (for example, indexed sequential file)

In addition, the NIST Workshop Agreements define the following document types: (1) NBS-6 (sequential file with a wide choice of primitive encodings), (2) NBS-7 (random access file), (3) NBS-8 (indexed sequential file), and (4) NBS-9 (set of file firectory entires). NBS-6, NBS-7, NBS-8 and NBS-9 are all optional in GOSIP. It is likely that NBS-9 will be superseded by the specifications of the FTAM Filestore Management Addendum when that Addendum achieves IS status.

There are two FTAM service types defined. One is internal; this supports the error recovery protocol. Errors are apparent to the file service user, the user is allowed to directly control error recovery procedures, there are four classes of errors defined, and all the functional units defined in the standard are included. The other is called external; in this situation, the file service user has no awareness of error detection and recovery, it is dependent upon the files quality of service level, and it includes all functional units except restart and recovery.

Three kinds of attributes defined in the NIST Workshop Agreements are: kernel, storage, and security. Each group contains both file and activity attributes. The group titles indicate their functional descriptions. There is limited concurrency control provision within the FTAM agreement. All functional units are supported except restart and recovery.

The NIST Workshop Agreements [NIST 1] have specific information on parameters as well as how information is negotiated. An FTAM implementation may act in any of four roles: initiator-sender, initiator-receiver, responder-sender, and responder-receiver. When data is actually being exchanged, one side is the sender and the other side is the receiver. This is independent of the initiator-responder relationship. In addition, the NIST Workshop Agreements describe Implementation Profiles, which are created so the user can conveniently specify the functionality required. The Profiles are: simple file transfer, positional file transfer, full file transfer, simple file access, full file access, and management.

These Implementation Profiles are expressed in terms of document types, attributes, and service classes. The Implementation Profiles described in the agreements support the functions of file transfer, file access, and management, and cover all possible situations of interest in basic FTAM capability.

The FTAM Phase Two agreements are upwardly compatible with future FTAM phases, and specify both intiator and responder roles. In addition, these agreements describe both sender and receiver features, support both NIST and FTAM document types, and include concurrency, requested access, and security considerations. The kernel group of attributes is required in these agreements, but all service classes are included.

FTAM Phase Three is an enhancement to Phase Two; Phase Three provides augmented document types, plus restart and recovery capabilities. Phase Three is essentially backwardly compatible to Phase Two, with minor exceptions detailed in the NIST Workshop Agreements. FTAM Phase Three functionality is scheduled for inclusion in GOSIP Version 3.

A.3.2 FTAM Support-Application Layer

The ACSE [ISO 12-13] standards specify a protocol and service common to any application. Since these services of connection establishment and release, as well as identification of source and recipient, are not particular to one application, they were included in a separate standard. This standard is meant to be referenced by all applications, and to provide a framework in which different applications can co-exist.

Application Layer standards define the procedures and the types of information necessary to enable interworking among distributed application processes. The Presentation Layer standards provide mechanisms for defining and selecting the encoding rules for representing the information to be communicated. The data elements defined by the Application Layer standards are abstract definitions of the information to be communicated. It is likely that data elements will be represented "locally" in each system according to different conventions. The conventions for representing information in a computer system are collectively referred to as the syntax of the information. Each system is said to represent the information in its local syntax.

To be meaningful, the procedures and types of information used by application processes to interwork must be encoded according to the same rules. Although it is not necessary that both systems use the same local syntax, it is necessary that they agree on the concrete syntax rules for encoding the information to be transferred. The concrete syntax used in the transfer is called the transfer syntax. In a communication, the transfer syntax may correspond to the local syntax of one or both of the systems involved, or it may be different from that of both systems. What is essential is that both systems agree on the transfer syntax and are capable of transforming information from their local syntax to the agreed transfer syntax.

Association Control Service Elements may be used to perform certain generic functions for the FTAM activity; these functions include setting up an association, terminating an association, and error control. These ACSEs and corresponding FTAM elements are carried by the Presentation Layer protocol.

Other Application Layer standards are important to FTAM besides the ACSE service and protocol. For instance, the emerging CCR (Commitment, Concurrency, and Recovery) standard deals with the following repetitive actions. Commitment specifies the completeness of actions possible on a particular data set, concurrency deals with controlling simultaneous access to a file, and recovery specifies actions necessary to

recreate the status of an application activity.

A.3.3 FTAM Support-Presentation Layer

The Presentation Layer standards [ISO 14-15] have mechanisms enabling applications to define and select the transfer syntax for their communication. The Presentation context is negotiated by functions in the Presentation Layer on behalf of the two application processes from the possible set of transfer syntaxes each system can support. During the communication, functions in the Presentation Layer may agree to change the Presentation context, selecting a new one as required by Application Layer standards. The Presentation Layer performs functions that are requested sufficiently often to warrant finding a general solution for them, rather than letting each user solve the problem.

An example of a transformation service that can be performed at the Presentation Layer is text compression. Most applications do not exchange random binary bit strings; they exchange information such as names or amounts. The Presentation Layer could accept ASCII strings as input and produce compressed bit patterns as output.

The Presentation Layer supports FTAM in terms of establishing and releasing a Presentation context, as well as carrying FTAM and ACSE information between machines. The Presentation address also binds different application processes. Context refers to the syntax in which information is transferred. What the Presentation Layer does for FTAM is to define the allowable syntaxes for FTAM information and control their use.

A.3.4 FTAM Support-Session

The Session Layer provides functions to interconnect or bind two application processes in a logical communicating relationship and to organize and synchronize their dialogue. This is done by providing mechanisms to establish and release Session connections. A Session connection is an agreement between two application processes to engage in a controlled dialogue for the purpose of exchanging data. It is by means of Session connections that application processes can exchange data between them. By the mechanism of the Session connection, application processes can send data and the receiving system can associate it with the intended application process.

The Session connection can be viewed as a connection between the two application processes across the Session Layers of the two end systems. It must be remembered, however, that the Session connection depends on the connection established at lower layers to carry out the Session Layer functions. It depends on these connections to transport data and protocol information. During the connection establishment the two application processes agree on the rules of dialogue to be used in the communication between them. The concept of a dialogue in the Session Layer is similar to that known from human communication. One type of dialogue is characterized by information flowing in only one direction. A second type of dialogue is characterized by a two-way flow of information that is controlled so information flows only in one direction at any given time.

The Session Layer manages the FTAM connection and synchronizes the FTAM data flow. The Session Layer marks (or checkpoints) the FTAM data, so that transmission can restart at a convenient point if an error occurs at the lower layers.

A.4 Message Handling Systems Tutorial

This section gives a general description of the services provided by MHS to the user. For more information, see the References portion of this Guide.

A.4.1 Functional Model

The Message Handling Systems application specified in GOSIP is based on the CCITT 1984 Recommendations. CCITT used the functional model shown in figure 29 to develop those recommendations.

The Message Handling System allows users to communicate by exchanging messages. There are two major MHS components - the Message Transfer System (MTS) and the cooperating User Agents. The Message Transfer System is composed of a series of Message Transfer Agents (MTAs) that are responsible for relaying the message from the originator's User Agent to the recipient's User Agent. The MTA serving the recipient need not be active when the message leaves the originator's MTA; the message can be stored at an intermediate MTA until the recipient's MTA becomes operational. Intermediate MTAs can also perform Application-Layer routing based on address information contained in the message.

The MTAs can be managed by different organizations or administrations. An administration is either the central Postal Telephone and Telegraph (PTT) service in a country or, in the United States, a common carrier recognized by the CCITT. The collection of MTAs and UAs owned and operated by an Admini- stration is called an Administration Management Domain (ADMD). The collection of MTAs and UAs owned and operated by a private organization is called a Private Management Domain (PRMD). Figure 30 shows how PRMDs can cooperate with ADMDs to provide the message transfer service. All ADMDs must comply with the CCITT Recommendations. PRMDs that wish to use a message transfer system provided by an ADMD must comply with the CCITT Recommendations at the point of interconnection.

CCITT has mandated that Transport Class 0 and the Connection-Oriented Network Service (CONS) be used in message systems provided by ADMDs. The NIST Workshop Agreements allow PRMDs to use either Transport Class 0 and CONS or Transport Class 4 and either CONS or the Connectionless Network Layer Protocol (CLNP) at layers 3 and 4. Transport Class 4 and the CLNP are the alternatives most widely implemented in the United States. If a PRMD that does not use Transport Class 0 and CONS wishes to interoperate with an ADMD, a relay MTA containing both Transport and Network Layer implementations must be provided by either the PRMD or the ADMD.

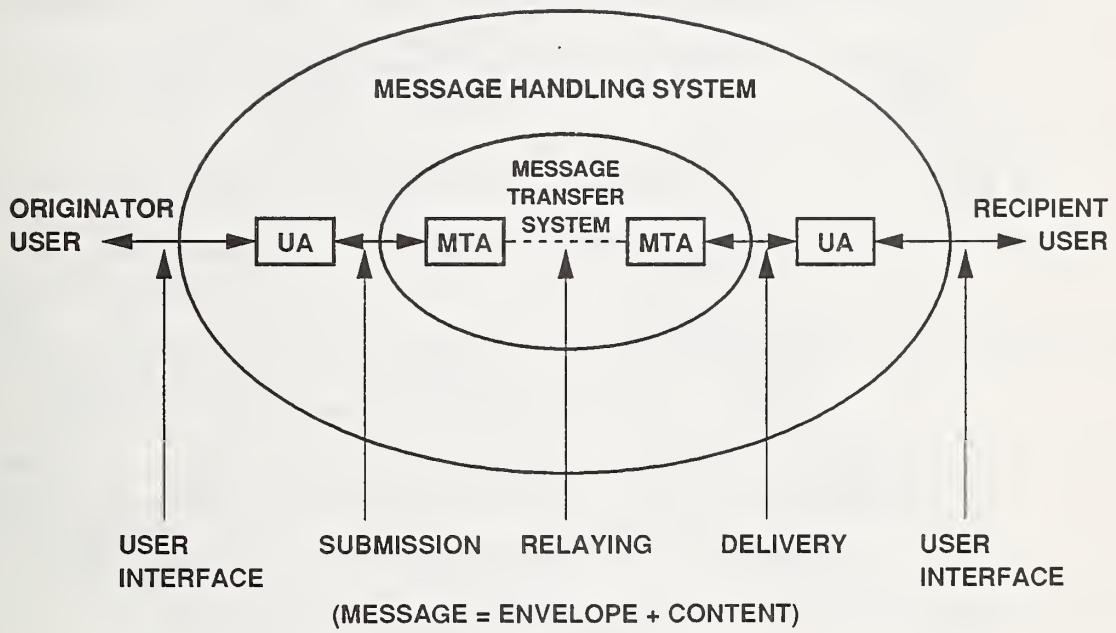
User Agents are the other major components of a Message Handling System. User Agents have many functions that are outside the realm of standardization. The originator's User Agent assists in the creation and editing of a message; the recipient's User Agent stores the message until the recipient chooses to read it and can use certain message fields to determine the display order. However, the message submission and delivery interaction with the MTA must be standardized.

The originator's User Agent must supply to the MTS the message content, the address(es) of the message recipients, and the MTS services that are being requested. The message content is the information that the message originator wants transferred to the message recipient. The address and service request data are placed on the message envelope and used by the MTS to deliver the message.

User Agents can be implemented either in the same system as the MTA or remotely located from the MTA. A remote or stand-alone UA can be under the control of an ADMD, a PRMD vendor, or an organization that provides no message transfer services. Since the UA-MTA message submission and delivery interactions involve a transfer of responsibility for delivering a message, there must be a protocol between the remote UA and MTA to ensure that the transfer of responsibility occurs.

There can be many different types of User Agents. The Message Transfer System can be used to transfer data unrelated to a personal message. It could be a binary bit stream of process control information. As long as the recipient's User Agent can interpret the data sent by the originator's User Agent, meaning-

Reprinted courtesy of
OMNICOM Corporation.



UA = USER AGENT
MTA = MESSAGE TRANSFER AGENT

FIGURE 29
MHS FUNCTIONAL MODEL

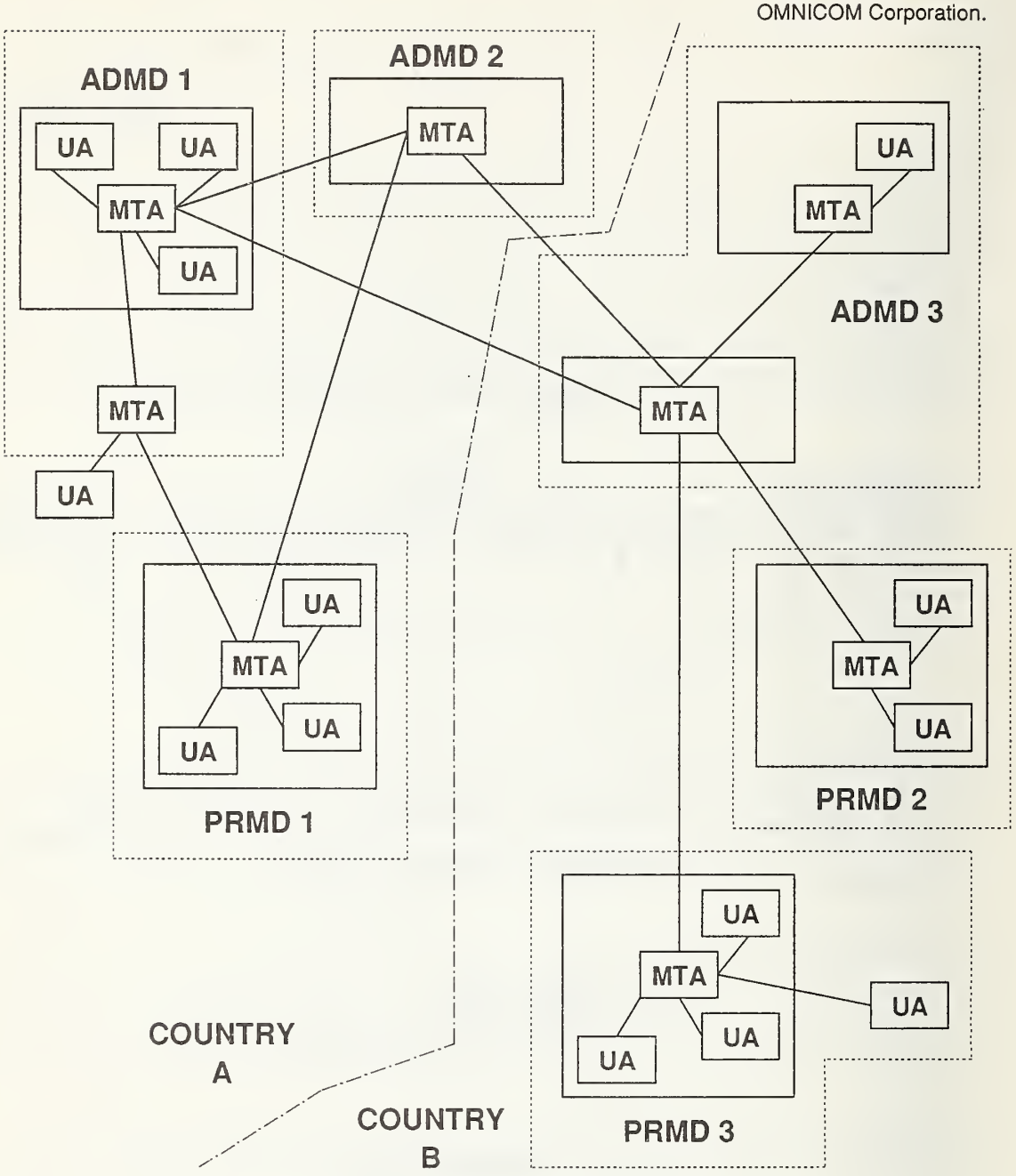


FIGURE 30
X.400 - ADMINISTRATION AND
PRIVATE MANAGEMENT DOMAINS

ful communication can occur. The Message Transfer System does not examine the message content unless the User Agent requests that the content be converted from one format to another before delivery. CCITT recognized that, although there were many potential User Agents that could use the message transfer services, the most common use of the Message Transfer System would be to send a personal message from an originator to one or more recipients.

CCITT called the User Agent that provides this service an Interpersonal User Agent and standardized that functionality in the 1984 Recommendations. Although CCITT did not standardize other types of User Agents, they can also use the services of the Message Transfer System as long as they comply with the rules of interaction when submitting or accepting delivery of a message.

A.4.2 Message Transfer System

The Message Transfer System provides basic services to User Agents; these are listed below.

A. Message Identification - A unique ID is assigned to each message. This message ID is used by the MTS to reference messages in delivery and nondelivery notifications.

B. Submission and Delivery Time Stamp - the MTS stamps the time that it accepted responsibility for delivering a message and the time that it fulfilled that responsibility.

C. Non-Delivery Notification - a notification is provided to the originator UA if a message cannot be delivered to any recipient UA.

D. Encoded Information Type Conversion - the originating UA can specify to the MTS the encoded information type of the message being submitted and the MTS can indicate to the recipient UA whether it converted the encoded information when it delivers a message.

E. Content Type Indication- this service enables the originating UA to indicate the content type of the message being submitted. An example of a content type is an Interpersonal Message (IPM).

The service elements below can be selected by the UA on a per-message basis.

A. Multi-destination delivery - the originating UA can request that a message be delivered to more than one recipient.

B. Delivery Notification - the originating UA may request a notification of delivery to each recipient UA.

C. Grade of delivery - three levels of priority processing are provided: normal, urgent, and nonurgent.

D. Deferred delivery - the originating UA may request that a message not be delivered before a certain time. The message is held at the originator's MTA until the delivery time is reached. The deferred delivery request can be cancelled by the originating UA during that interval.

E. Conversion prohibition - the originating UA may prohibit conversion of the encoded information in a message. A non-delivery notification will result if the message cannot be delivered to the recipient UA.

F. Alternate Recipient Allowed - the originating UA can allow this message to be delivered to an alternate UA if there is not an exact match in the Personal Name attribute. The alternate UA is normally a service desk that will manually process the message. The MTS is not required to provide these alternate UAs. If one is not provided, a non-delivery notification will occur.

G. Disclosure of other recipients - the originating UA can instruct the MTS to disclose the names of the other recipients of a multi-recipient message. The originating MTA need not provide the ability to request

this service to the originating UA but, if this service element appears in the message, it must be supported by the recipient MTA.

Additional MTS service elements appear in the CCITT 1984 Recommendations but the NIST Workshop Agreements [NIST 1] do not mandate that they be supported.

A.4.3 Interpersonal Message Service

The Interpersonal Message Service is provided by the class of cooperating UAs called IPM UAs. This service enables a user to send an interpersonal message to one or more recipients and have it received by those recipients. The IPM service is built upon and uses the services of the Message Transfer System.

The interpersonal message contains a header and body. The interpersonal message header contains service elements which facilitate efficient processing of the message by the recipient's UA. The body of the interpersonal message is the information that the message originator wishes to convey to the message recipient. The NIST Workshop Agreements designate the IPM service elements in the interpersonal message header as falling into the following categories.

The service elements below are required in all interpersonal message headers.

A. Interpersonal Message ID - this service element is used by IPM UAs and users to uniquely identify the interpersonal message. The particular method by which this identifier is generated is a local matter. Note that this identifier refers to the message content and is not used by the MTS to reference messages.

B. Originator indication - this service element allows the identity of the originator to be conveyed to the message recipient(s).

The service elements below must be able to be generated upon user request.

A. Primary and Copy Recipients Indication - this service element allows the originator to provide the names of one or more users who are the intended primary and copy recipients of the message. Primary recipients are those who might be expected to act on the message; secondary recipients may be sent the message for information only.

B. Subject Indication - this service element identifies the subject of the message.

C. Replying Interpersonal Message Indication - this service element identifies the message to which this message is a response.

The IPM service need not offer the ability to generate the following service elements to users but if they do appear in an interpersonal message, the receiving UA must recognize them and convey the information to the message recipient. One of the service elements, Blind Copy Request Indication, requires additional processing by the recipient's UA.

A. Authorizing Users Indication - this service element enables the originator to indicate to the recipient the names of one or more persons who authorized the sending of the message.

B. Blind Copy Recipients Indication - this service element allows the originator to provide the names of one or more users who are intended recipients of the message but whose names are not disclosed to either the primary or copy recipients.

C. Cross-Referencing Indication - this service element allows the originator to relate this message to one or more previously sent messages.

D. Obsoleting Indication - this service element allows the originator to indicate that one or more previously sent messages are obsolete.

E. Expiry Date Indication - this service element allows the originator to state the date and time at which the interpersonal message will be obsolete.

F. Reply Request Indication - this service element enables the originator to request that a recipient send an interpersonal message in response to this message. The originator can specify the names of one or more users to whom the reply should be sent and the date by which the reply is required.

G. Importance Indication - this service element allows the originator to indicate his/her assessment of the importance of the message being sent. Three levels of importance are defined: low, normal, and high.

H. Sensitivity Indication - this service element allows the originator to specify guidelines for the relative security of the message upon its receipt. Three levels of sensitivity are defined as follows:

Personal (the interpersonal message is sent to the recipient as an individual, not because of the position that the recipient has in an organization),

Private (the interpersonal message contains information that should be seen only by the recipient), and

Company-confidential (the interpersonal message contains information that should be handled according to company security procedures).

I. Auto-Forwarded Indication - an auto-forwarded message is one that has been forwarded by a recipient UA without user intervention. A new-header encapsulates the original message. This service element allows the recipient to determine that auto-forwarding has taken place and can be used by the recipient UA to prevent additional auto-forwarding and thus act as a loop control mechanism.

Additional IPM service elements appear in the CCITT 1984 Recommendations but the NIST Workshop Agreements do not mandate that they be supported.

A.4.4 Naming and Addressing

In the context of electronic mail, a name is the term by which originators and recipients of messages identify each other. An address identifies an entity by specifying where it is, rather than what it is. An address has characteristics that help the MTS locate the recipient UA's point of attachment.

A name is formed by specifying a set of attributes and the associated values of those attributes. Table 5 gives an attribute list that can uniquely identify a user of the Message Handling System:

Table 5 - MHS Attribute List

Country = United States

Organization Name = ABC Corporation

Personal Name = John Taylor

The address of the message recipient consists of information required to deliver the message to an MHS implementation on a particular end system plus the information needed by the MHS implementation to deliver the message to the recipient's User Agent. The MHS implementation address includes the NSAP address plus the TSAP and SSAP selectors. The Personal Name attribute can be used alone or in conjunction with other attributes to locate the recipient's User Agent.

The CCITT has developed a standard for a directory service to perform the name-to-address mapping [CCITT 10]. An International Standard for directory services has been issued by the ISO/IEC [ISO 17].

Until directory service products are widely available, a method of performing the name-to-address mapping is needed.

The solution is to think of an address as a name that contains attributes that are used to locate the message recipient. Name attributes normally consist of information that the originator knows about the potential recipient of a message. Address attributes describe the architecture of the MTS and may be harder for users to remember but they can be used to route the message to the correct MTA.

Table 6 gives an example of how architectural attributes can be applied to the attributes in table 5 to assist in the message routing.

Table 6 - MHS Architectural Attributes

Country = United States

Administration Name = Public Mail System X

Private Domain Name = Private Mail System Y

Organization Name = ABC Corporation

Personal Name = John Taylor

A.5 VIRTUAL TERMINAL

This section gives a general description of the VT protocol and services.

A.5.1 Introduction

The ultimate goal of virtual terminal (VT) is that terminals, regardless of model or design, should be able to access application programs resident on either a local or remote system. Similarly, any application program should be able to communicate with any terminal, regardless of its model or design and whether it is resident on the same or a different system.

In reality, however, an application program expects to interact with a limited range of terminals. If the computer network is homogeneous, or if the terminal belongs to the specified range, communication is relatively easy. However, if the computer network is heterogenous, or the terminal does not belong to the range required by the application, communication becomes a problem.

A solution to this problem can be found in the Open Systems Interconnection (OSI) Virtual Terminal protocol, part of the OSI Application Layer. VT effectively isolates applications running on a wide variety of systems, irrespective of the supplier of terminal or host system.

In a world of heterogenous computer networks, it becomes obvious that accessing diverse computer systems through a single terminal (and vice versa) is no longer a desirable extra, but rather an urgent necessity. Neither can the commercial implications be ignored. VT means that people are no longer limited to buying from a single supplier after the initial installation of the original system. Hence, VT opens up intercommunication in a multi-vendor environment.

A.5.2 Virtual Terminal Goal

As its name suggests, VT solves the problem by simulating a real terminal, that is, by defining a virtual terminal. The virtual terminal attempts to represent the real terminal and the various operations possible on it. The VT standard provides for defining a variety of virtual terminals and abstract operations and hence can be tailored to suit the specific situation at hand. An illustration of this is given in figure 31.

With VT, a terminal can access an application program resident in a remote system, knowing that it does not have to belong to a limited range of terminals. Instead, it communicates with the virtual terminal agreed for that particular association, safe in the knowledge that the application program can communicate with the same virtual terminal Various abstract operations defined include: reading text from the virtual keyboard, writing text on the virtual screen, and moving a virtual cursor to a particular position on the virtual screen.

Similarly, an application program need not take into consideration those characteristics and control functions specific to the terminal with which it wants to communicate. Instead, the application program need only be concerned with communicating with the virtual terminal defined for that particular association, knowing that the real terminal can translate information on the virtual terminal into its own terminal-specific control functions and characteristics.

An interactive computer system can be designed to use the generalized functions of the Virtual Terminal Protocol (VTP) when communicating with terminals, thus, an application will be independent of any particular design of terminal. A terminal will generally include some conversion (or "mapping") between the virtual terminal functions and those of the actual terminal hardware. Designs of terminals may differ in the form of the actual hardware provided and in the way in which they are mapped to the virtual terminal functions; the latter is all that is "known" to the application.

A.5.3 Classes of Terminals

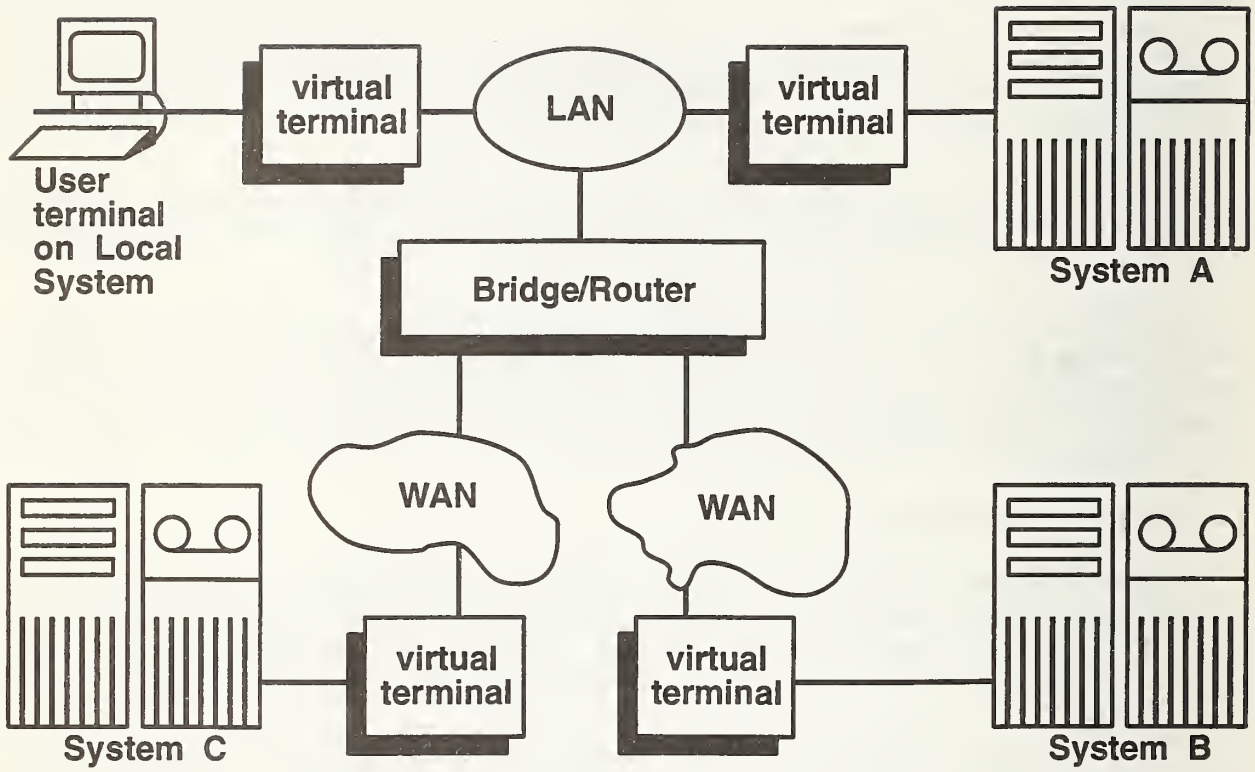


FIGURE 31
VT SCENARIO

The plans for the development of OSI Virtual Terminal Standards envisaged a number of classes of terminal each characterized by the type of data to be displayed and manipulated. There is informal agreement that the possible classes consist of:

1. Basic: data consisting of rectangular arrays of characters.

2. Forms: data consisting of characters arranged into fields of variable size and shape with the manipulation of content controllable for each field. These are sophisticated terminals with built-in processors, and supporting display-oriented applications that use shared data structures (either synchronous or asynchronous).

3. Graphics: data representing "computer graphics" elements, such as lines and circles, as covered by the Graphical Kernel System (GKS) standard (ISO 7942) and related standards.

4. Text; data representing document structures as covered by the Office Document Architecture (ODA) standards (ISO 8613).

5. Image: data representing images composed of arrays of dots ("pixels").

6. Page mode: typically CRT terminals that can display 25 lines of 80 characters each.

7. Scroll mode: no built-in processors or local editing capability; to communicate with the network, a PAD (packet assembler-disassembler) is used.

It is also intended that there should be a standard covering Terminal Management; this is intended to provide a common framework for the individual classes such that their operation can be coordinated and the resources of a real terminal shared between different classes (e.g., by the use of "windows") if desired.

To date, work has concentrated upon the Basic class, but the scope of this work has been expanded to include the Forms class

A.5.4 Concepts and Components of VT

The VT standards are in the form usual for OSI standards in that there is:

(1) a service definition (ISO 9040) [ISO 7] which defines what is communicated (in this case it defines both a set of terminal communication services and the terminal functions and parameters conveyed by these services), and (2) a protocol specification (ISO 9041) [ISO 8] which specifies how the services are provided.

For two VT-users to communicate there are various components that come into play. These are shown in figure 32.

The terminal driver and application program are parts of the VT-user that invoke the functionality of the VT service provider. The local mapping is that part of the VT-user that is responsible for translating between the VT service provider and the real terminal driver or application program, that is, for mapping from terminal-specific "language" to common VT "language," and vice versa.

The virtual terminal (abstract representation of the real terminal) is seen as consisting of several parts, all of which reside in a shared (that is, conceptually shared) data area known as the Conceptual Communications Area (CCA) For consistency, it is necessary that both VT-users keep local copies of the CCA.

The CCA can be regarded as a group of data structures and a "set of rules" to which the real terminal and the application program have agreed to comply for the lifetime of a particular VT-association. Both the group of data structures and the "set of rules" are incorporated into the local mapping component of the VT-user to aid in the translation process. The CCA is examined in full later.

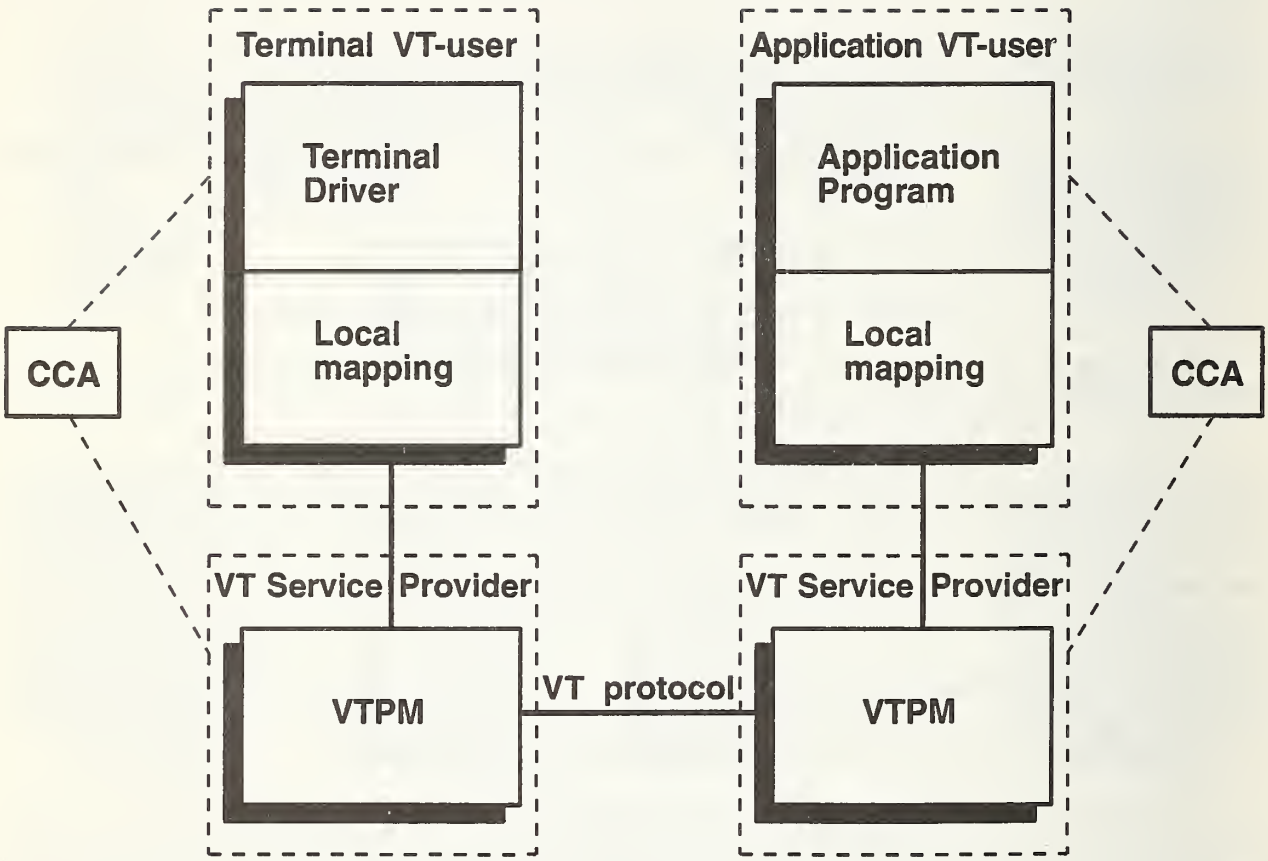


FIGURE 32
COMPONENTS OF VT COMMUNICATION

The VT Service Provider provides the VT functionality for the VT-users. It is responsible for:(1) establishing the initial VT environment in which all VT communications take place, (2) generating VT messages with the appropriate parameters, when called upon to do so by the VT-user, (3) decoding incoming VT messages and presenting this information to the VT user, (4) providing the functionality for the parsing and formatting of Virtual Terminal Protocol Data Units (VTPDUs), (5) implementing the VT protocol machine (VTPM), and (5) using the functionality of the lower layers as defined by the VT standard.

The essence of the VT protocol is that it provides a means to keep both the local and remote virtual terminal in synchronization.

The CCA has no physical existence; it is simply a group of data structures and a set of rules to which the Application Program and Real Terminal have agreed to comply. These rules are negotiated at association set-up when the virtual terminal is negotiated. The CCA contains various entities which model the terminal:(1) a Conceptual Data Store (CDS) containing one or more Display Objects, for S-mode or A-mode. These display objects model a screen/ keyboard, (2) an access control store (ACS) which keeps track of access rights, (3) a control, signalling and status store (CSS) containing zero or more control objects, (4) zero or more device objects which model real devices, and hence aid the mapping between display objects and a real device, (5) a data structure definition (DSD) which contains the object type definitions for the display, control and device objects and other virtual terminal environment (VTE) parameters, and (6) a reference information store (RIS) containing reference information objects (RIOS).

A display object is an abstract object used to model the exchange of graphic information. It is used to model devices such as the screen or keyboard. It allows real events which occur on a real terminal to be represented on the virtual terminal as abstract events.

Display objects are defined by one-, two-, or three-dimensional arrays of character box graphic elements. Each of the latter has two types of attribute: primary and secondary. The primary attributes describe the identity of a character and its position in the display object. The secondary attribute describes the element's characteristics, e.g., background color, foreground color, emphasis, and font.

Structure may be imposed on display objects by defining blocks and fields. A block is a simple subdivision of a display to aid in addressing. Addresses can be specified relative to the current block. A field is a non-overlapping area of a display object used for the validation of human user entry. The validation is done locally, thus saving the time, capacity, and resources which would be wasted if validation were done remotely across a network.

Device objects are used to model characteristics of real devices and are intended to assist in mapping display objects to these real devices.

Control Objects are abstract objects which can be used to model aspects of real terminals such as bells, or to handle control information. Control objects can also be used for modeling the exchange of any unstructured information of a single type and are not limited to information of a control nature (although this is their primary application).

Another type of control object is called a structured control object. These are used to define fields and to control data entry to fields.

A.5.5 Access Rights and Modes of Operation

A virtual terminal can operate in one of two modes: asynchronous mode (A-mode) and synchronous mode (S-mode). The access rights differ depending upon which mode of operation is in use.

In A-mode there are two display objects, depicting the asychronous nature of operation of the terminal. These display objects can be used to model the screen and keyboard. One display object can be updated by the application, and models a screen which is controlled by the application. The other display object can be

updated by the terminal end, and models a screen which is controlled by the keyboard.

Each display object has an access right, which is assigned to it for the duration of the VT Association. These access rights give one VT-user or the other the sole right to update that particular display object. The access rights are called Write Access Connection Initiator (WACI) and Write Access Connection Acceptor (WACA). The VT-user who starts the communication is known as the Initiator VT-user and the other VT-user is known as the Acceptor VT-user. A display object with the WACI access right can only be updated by the Initiator VT-user. A display object with the WACA access right can only be updated by the Acceptor VT-user.

In A-mode, there can be zero or more control objects. Each control object has an access right, which is assigned to it for the duration of the VT association. These access rights give one VT-user or the other the sole right to update that particular object.

Control objects can be assigned one of four access rights: Write Access Connection Initiator (WACI), Write Access Connection Acceptor (WACA), Not Subject to Access Control (NSAC), and no-access. A control object with the WACA access right can only be updated by the Acceptor VT-user. A control object with the no-access right cannot be accessed (whatever value it has is permanent, and may not be changed).

In S-mode there is only one display object, and there is only one access right that may govern it-Write Access Variable (WAVAR).

With WAVAR, the right to access a display object passes back and forth between the two users. This is intended to model the half-duplex nature of synchronous terminals.

Similarly, WAVAR access rights to control objects also conform to the half-duplex characteristics of synchronous terminals.

If, however, the enhanced access rules are employed for a particuar VT-association, the WACI and WACA non-reassignable access rights may be used with the WAVAR access right. Hence, a control object with the WACI access right may only be updated by the Initiator VT-user, and then only if he is in possession of the token. A control object with the WACA access right may only be updated by the Acceptor-VT user, and only when he is in possession of the WAVAR access right. In S-mode, there are zero or more control objects. There are two access rights that may govern them: WAVAR and no-access.

A.5.6 Profiles

Groups of parameters that are frequently used together to describe a Vitrual Terminal environment (VTE) are grouped together to form a VT profile. A VT profile is a set of parameters that describes a VTE, with values already assigned to the parameters. This VT profile is then given a name, and is henceforth referenced by this name. So, at association set-up (when a communication is established), a user suggests using a particular profile, rather than negotiating all the individual parameters.

The TELNET profile supports a simple line at a time or character at a time dialogue, and enables an application level gateway supporting Internet Telnet and ISO VT interoperation. The Transparent Profile supports the exchange of uninterpreted sequences of characters. This includes support of VT-users who wish to control terminals directly through the use of embedded control characters and escape sequences.

The Forms profile is intended to support forms-based applications with local entry and validation of data by the terminal system.

GOSIP defines 1) simple systems and 2) forms-capable systems for procurement pruposes. A simple system provides the functions of a TTY-compatible device, and supports the TELNET profile with the A-mode of operation. A forms-capable system supports functions such as "cursor movement," "erase screen," and "field protection"; it supports the Forms profile (S-mode).

When VT profiles are not sufficient, life becomes more complicated for an application. Those VT services that are viewed as being essential are grouped together to form the VT Kernel. All the other groups of services (functional units) are named after the type of activity on which they are based. When an Application Layer product is stipulating its basic requirements, it does so in terms of functional units, that is, it specifies what functional unit it requires from the layers below. Functional units are negotiated between two peer entities at connection establishment.

There are dependencies between some of the VT functional units. Multiple Interaction Negotiation cannot be selected without Switch Profile Negotiation. Fields cannot be selected without Structured Control Objects. Reference Information Objects cannot be selected without Structured Control Objects.

Apart from supporting individual VT functional units, some Presentation and Session functional units are required for VT to work at all. For example, without the Session functional unit, Major Synchronize, profile switching is not possible, but without the Session functional unit Typed Data, VT cannot operate at all. Those Presentation and Session functional units mandatory for VT's operation are: Presentation-Kernel, and Session-Kernel, Typed Data, Full-Duplex (for A-mode), and Half-Duplex (for S-mode).

Work is underway in the NIST Workshop on a mapping of the X-Window user interface capabilities to OSI.

APPENDIX B

ADDITIONAL OSI REFERENCES

Information provided in this Appendix consists of additional references for OSI standards ard related material, and where to obtain this documentation. Agencies may use the addresses indicated to order this information, or it may be ordered from OMNICOM, Inc. at the address below.

OMNICOM, Inc.
115 Park Street, SE
Vienna, VA 22180
(703) 281-1135

Material is presented in this Appendix by group (i.e., CCITT, ISO), and by particular subjects or layers within a group (i.e., Network Layer, Transport Layer). References appearing in the REFERENCES section of this Users' Guide do not appear in this Appendix. For ISO and CCITT references, information is current as of June, 1990. This is not a complete list of OSI-related material; for additional sources of information, contact any one of the organizations given in this Appendix.

CCITT
(Consultative Committee for International Telegraph and Telephone)

Layer-Independent

CCITT Recommendation X.200, (Red Book, 1984), Reference Model of Open Systems Interconnection

Physical layer

CCITT Recommendation V.35 - Data Transmission at 48 Kilobits/sec using 60-108 KHz Group Band Circuits

Data Link Layer

CCITT Recommendation X.212, Data Link Service Definition for CCITT Applications

Network Layer

CCITT Recommendation X.213, Network Service Definition for CCITT Applications

Transport Layer

CCITT Recommendation X.214, Transport Service Definition for Open Systems Interconnection for CCITT Applications.

CCITT Recommendation X.224, Transport Protocol Profile for Open Systems Interconnection for CCITT Applications.

Session Layer

CCITT Recommendation X.215, Session Service Definition for Open Systems Interconnection for CCITT Applications.

CCITT Recommendation X.225, Session Protocol Profile for Open Systems Interconnection for CCITT Applications.

Presentation Layer

CCITT Recommendation X.216, Presentation Service Definition for Open Systems Interconnection for CCITT Applications.

CCITT Recommendation X.226, Presentation Protocol Profile for Open Systems Interconnection for CCITT Applications.

Application Layer

CCITT Recommendation X.217, Service Definition for the Association Control Service Element

CCITT Recommendation X.227, Protocol Specification for the Association Control Service Element

CCITT Recommendation X.218, Reliable Transfer, Part 1: Model and Service Definition

CCITT Recommendation X.228, Reliable Transfer, Part 2: Protocol Specification

CCITT Recommendation X.219, Remote Operations, Part 1: Model, Notation, and Service Definition

CCITT Recommendation X.229, Remote Operations, Part 2: Protocol Specification

CCITT Recommendation X.501, The Directory, Part 2: Information Framework

CCITT Recommendation X.511, The Directory, Part 3: Access and System Services Definition

CCITT Recommendation X.518, The Directory, Part 4: Procedures for Distributed Operation

CCITT Recommendation X.519, The Directory, Part 5: Access and System Protocols Specification

CCITT Documents may be obtained from:

International Telecommunications Union
Place des Nations, CH 1211
Geneva 20, Switzerland

or

United Nations Bookstore
Room GA 32B
United Nations Plaza
New York, NY 10017

==========

EIA (Electronic Industries Association)

Physical Layer

Interface Between Data Terminal Equipment and Data Communication Equipment Employing Serial Binary Data Interchange, EIA-232D

Application Layer

Manufacturing Messaging Service for Bi-directional Transfer of Digitally Encoded Information, Part 1: Service Specification, RS 511, 1986

Manufacturing Messaging Service for Bi-directional transfer of Digitally Encoded Information, Part 2: Protocol Specification, RS 511, 1986.

==========

IEEE (Institute of Electrical and Electronics Engineers, Inc.)

Media Access Control (Physical Layer)

IEEE Standard for Local Area Networks: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) and Physical Layer Specification, ANSI/IEEE Standard 802.3 - 1985, Institute of Electrical and Electronics Engineers, 345 East 47th St., New York, NY 10017, 1985.

IEEE Standard for Local Area Networks: Token-Passing Bus Access Method and Physical Layer Specification, ANSI/IEEE Standard 802.4 - 1985, Institute of Electrical and Electronics Engineers, 345 East 47th

St., New York, NY 10017, 1985.

IEEE Standard for Local Area Networks: Token-Ring Access Method, ANSI/ISEE Standard 802.5 - 1985, Institute of Electrical and Electronics Engineers, 345 East 47th St., New York, NY 10017, 1985.

Data Link Layer

IEEE Standard for Local Area Networks: Logical Link Control, ANSI/IEEE Standard 802.2 - 1985, Institute of Electrical and Electronics Engineers, 345 East 47th St., New York, NY 10017, 1985.

==========

ISA (Instrumentation Society of America)

Instrumentation Society of America: Proway-LAN, ISA-S72.01, 1985.

Proposed Instrumentation Society of America Standard: Process Control Architecture, dS S72.03, 1987.

==========

ISO (International Organization for Standardization)

Layer-Independent

Information Processing Systems - Open Systems Interconnection - Reference Model, ISO 7498-3, Naming and Addressing.

Information Processing Systems - Open Systems Interconnection - Reference Model, ISO 7498-4, Management Framework.

ISO 7498-1/Addendum 1: Connectionless Data Transmission

ISO 7498-1/PDAD2: Multi-Peer Data Transmission

ISO DIS 9646, OSI Conformance Testing Methodology and Framework

ISO DIS 9834, Procedures for Specific OSI Registration Authorities

ISO 8807: LOTOS - A Formal Description Technicue Based on an Extended State Transition Model

ISO 9074: ESTELLE - Formal Description Technique Based on an Extended State Transition Model

ISO CD 10181-1: OSI Security Model, Part 1: Security Framework

ISO CD 10181-2: OSI Security Model, Part 2: Authentication Framework

Multi-Layer Standards (Profiles)

ISO TR 10000-1: International Standardized Profiles, Part 1: Texonomy Framework

ISO TR 10000-2: International Standardized Profiles, Part 2: Taxonomy of Profiles

Physical Layer

ISO 2110, 25-Pin DTE-DCE Interface Connector and Pin Assignments

ISO 4902, 37-Pin DTE-DCE Interface Connector and Pin Assignments

ISO 4903, 15-Pin DTE-DCE Interface Connector and Pin Assignments

ISO 2593, 34-Pin DTE-DCE Interface Connector and Pin Assignments

ISO 8481, DTE to DTE Physical Connection Using X.24 Interchange Circuits With DTE-Provided Timing

ISO 9314-1, FDDI, Part 1: Physical layer Protocol

Data Link Layer

ISO 8886, Data Link Service Definition

ISO 3309, High-Level Data Link Control (HDLC)-Frame Structure

ISO 4335, HDLC - Consolidation of Elements of Procedures

ISO 7776, HDLC - Description of the X.25 LAPB-compatible DTE Data Link Procedures

ISO 7809, HDLC-Consolidation of Classes of Procedures

ISO 7478, Multi-Link Procedures

ISO 8471, HDLC Balanced Classes of Procedures

ISO 8885, HDLC - General Purpose XID Frame Information Field Content and Format

ISO 1745, Basic Mode Control Procedures for Data Communication Systems

ISO 1177, Character Structure for Start/Stop and Synchronous Character Oriented Transmission

ISO 2629, Basic Mode Control Procedures - Conversational Information Message Transfer

ISO 8802-1, Local Area Networks, Part 1: Introduction

ISO 8802-2, Local Area Networks, Part 2: Logical Link Control

ISO 9314-2, FDDI, Part 2: Medium Access Control

Network Layer

Information Processing Systems-Open Systems Interconnection-Network Service Definition, IS 8348

Information Processing Systems-Open Systems Interconnection-Addendum to the Network Service Definition Covering Connectionless Data Transmission, IS 8348/AD1

Information Processing Systems-Open Systems Interconnection-Addendum to the Network Service Definition covering Network Layer Addressing, IS 8348/AD2

Information Processing Systems-Open Systems Interconnection-Internal Organization of the Network Layer, IS 8648

Information Processing Systems-Open Systems Interconnection-Addendum to IS 8473-Provision of the Underlying Service Assumed by ISO 8473, ISO TC 97/SC 6 N 3453

Information Processing Systems-Open Systems Interconnection, Working Draft, End System to Intermediate System Routing Exchange Protocol for Use in Conjunction with ISO 8473 ISO TC 97/SC 6 N 4053

Information Processing Systems-Open Systems Interconnection-Data Communication-X.25 Packet Level Protocol for Data Terminal Equipment, IS 8208

ISO 8878, Use of X.25 to Provide the Connection-Oriented Network Service

ISO 8881, Use of the X.25 Packet Layer Protocol in LANs

ISO 8880, Protocol Combinations to Provide and Support the OSI Network Service

ISO 9574, Provision of the OSI Connection-mode Network Service by Packet-Mode Terminal Equipment Connected to an ISDN

Transport Layer

Information Processing Systems-Open Systems Interconnection-Transport Service Definition, IS 8072

Information Processing Systems-Open Systems Interconnection-Transport Protocol Profile, IS 8073

IS 8602, Protocol for Providing the Connectionless-Mode Transport Service

Session Layer

Information Processing Systems-Open Systems Interconnection-Session Service Definition, IS 8326

Information Processing Systems-Open Systems Interconnection-Session Protocol Profile, IS 8327

IS 9548, Connectionless Session Protocol

Presentation Layer

Information Processing Systems-Open Systems Interconnection-Profile of Abstract Syntax Notation One (ASN.1), IS 8824

Information Processing Systems-Open Systems Interconnection-Profile of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1), IS 8825

7-bit Coded Character Set for Information Processing Interchange, ISO-646

Information Interchange - Representation of Local Time Differentials, ISO 3307

IS 9576, Connectionless Presentation Protocol Specification

Application Layer

Information Processing Systems-Text and Office Systems-Office Document Architecture (ODA) and Interchange Format-Part 1: General Information, IS 8613/1

Information Processing Systems-Text and Office Systems-Office Document Architecture (ODA) and Interchange Format-Part 2: Document Structures, IS 8613/2

Information Processing Systems-Text and Office Systems-Office Document Architecture (ODA) and Interchange Format-Part 3: Document Processing Reference Model, IS 8613/3

Information Processing Systems-Text and Office Systems-Office Document Architecture (ODA) and Interchange Format-Part 4: Document Profile, IS 8613/4

Information Processing Systems-Text and Office Systems-Office Document Architecture (ODA) and Interchange Format-Part 5: Office Document Interchange Format, IS 8613/5

Information Processing Systems-Text and Office Systems-Office Document Architecture (ODA) and Interchange Format-Part 6: Character Content Architecture, IS 8613/6

Information Processing Systems-Text and Office Systems-Office Document Architecture (ODA) and Interchange Format-Part 7: Raster Graphics Content Architecture, IS 8316/7

Information Processing Systems-Text and Office Systems-Office Document Architecture (ODA) and Interchange Format-Part 8: Geometric Graphics Content Architecture, IS 8613/8

Application Process–Computer Graphics–CGM/GKS

Information Processing Systems-Computer Graphics-Metafile (CGM) for the Storage and Transfer of Picture Description Information, Part 1: Functional Specification, IS 8632/1

Information Processing Systems-Computer Graphics-Metafile (CGM) for the Storage and Transfer of Picture Description Information, Part 2: Character Encoding, IS 8632/2

Information Processing Systems-Computer Graphics-Metafile (CGM) for the Storage and Transfer of Picture Description Information, Part 3: Binary Encoding, IS 8632/3

Information Processing Systems-Computer Graphics-Metafile (CGM) for the Storage and Transfer of Picture Description Information, Part 4: Clear Text Encoding, IS 8632/4

Information Processing Systems-Font and Character Information Interchange, IS 9541

Information Processing Systems-8-bit Single Byte Coded Graphic Character Sets, Part 1: Latin Alphabet Part 1, IS 8859/1

Information Processing Systems-Computer Graphics Functional Specification of the Graphical Kernel System (GKS), IS 7942

Information Processing Systems-Computer Graphics-Graphical Kernel System for Three Dimensions (GKS-3D), Functional Description, IS 8805

Information Processing Systems-Computer Graphics-Programmers Hierarchical Interactive Graphics System (PHIGS), IS 9592

Information Processing Systems-Computer Graphics-Interfacing Techniques for Dialogues with Graphical Devices (CGI), ISO TC 97/SC 21 N1179

Other Application Layer

ISO 8831, Job Transfer and Manipulation Concepts and Services

ISO 9545, Application Layer Structure

ISO DIS 9804, Definition of Application Service Elements - Commitment, Concurrency, and Recovery

ISO DIS 9805, Specification of Protocols for Application Service Elements - Commitment, Concurrency, and Recovery

ISO DIS 9595, Management Information Service Definition

ISO DIS 9596, Management Information Protocol Specification

ISO CD 9579, Remote Database Access

ISO 9066, Reliable Transfer

ISO 9072, Remote Operations

ISO DIS 10026, Transaction Processing

ISO 10035, Connectionless ACSE Protocol

ISO documents may be obtained from:

ANSI
ISO TC 97/SC 6 Secretariat
1430 Broadway
New York, NY 10018

==========

NIST (National Institute of Standards and Technology)

Local Area Networks: Baseband Carrier Sense Multiple Access with Collision Detection Access Method and Physical Layer Profiles and Link Layer Protocol, FIPS 107, NTIS, U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161

Interface Between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for Operation With Packet-Switched Data Communications Networks, FIPS 100, NTIS, U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161

Implementation Guide for ISO Transport Protocol, National Institute of Standards and Technology, ICST/SNA-85-18, 1985

Franx, C.;Mills, K., Open Systems Interconnection for Real-Time Factory Communications: Performance Results, Workshop on Factory Communications, National Institute of Standards and Technology, NBSIR 87-3516, 1987

NIST FIPS documents may be obtained from:

NTIS
U.S. Department of Commerce
5285 Port Royal Road
Springfield, VA 22181

Other NIST documents may be obtained from:

National Institute of Standards and Technology
Computer Systems Laboratory
Gaithersburg, MD 20899

ANSI
American National Standards Institute

Integrated Services Digital Network - Basic Access Interface for Use on Metallic Loops for Application on the Network Side of the NT-Layer 1 Specification, ANS T1.601-1988

Integrated Services Digital Network - Basic Access Interface at S and T Reference Points - Layer 1 Specification, ANS T1.605-1988

Carrier to Customer Installation - DS1 Metallic Interface, ANS T1.403-1989

APPENDIX C

NIST/OSI WORKSHOP PARTICIPANTS LIST

This Appendix gives a partial list of organizations participating in the NIST/OSI Workshop. The goal of this Workshop is to develop implementation agreements based upon emerging recognized international OSI standards. This list is arranged alphabetically, and includes both vendors, users, and other interested parties.

This list is taken from participant registrations according to NIST records since January 1987. If a participant has registered at least once for any Workshop during this period, that participant's organization should be represented on this list. NIST does not represent this list as being complete.

LIST OF WORKSHOP ATTENDEES

ACIS-Australian Unisys Center, ADCU/WE, Aeronautical Radio, AGFA Compugraphic, Ajou University (South Korea), Allen-Bradley, Allied-Signal, Allied Technologies, Ameritech, Analytic Sciences, Apollo, Apple Computers, Apple Computer-Europe, Applied Technologies, ARINC Research, Arix Corporation, Arthur Anderson, ASR Group, AT and T, Australian Ministry of Defense, Automated Office Systems, Bank of America, Banyan Systems, BBN Communications, Bechtel, Bell Atlantic, Bell Canada, Bell Communications Research, Bell Northern, Bell Southern, BNR, Boeing, Booz Allen, Bridge Communications, British Telecom, Bull, Cambridge University, Canon, Carnegie-Mellon, Case Communications, CCTA, CDSI, Chipcom, Cimage Corporation, Codex, Commission of European Community, Computer Consoles, Computing Unlimited, Computrol Corporation, Comsat, Concord, Consumers Software, Contel, Control Data, Convergent Technologies, COS, Cray Research, CSC, CSIRO, CTA Incorporated, D and F Communications, Danish Standards Association, Danish Telecom, Data Connection, Data General, Datapoint, Data Systems Analysts, Datatrend, David Taylor Research Center, DCEC, DEC, Defense Communications Agency, Defense Logistics Agency, Department of Agriculture, Department of Defense, Department of Education, Department of Energy, Department of Veterans' Affairs, DFN/GMD, DGM and S, Dialcom, Dupont, Eagle Technologies, Eastman Kodak, EDS, EEMSI, Electrical Engineering Group, Electricite de France, Enlon, Excelan, FAA, FBI, Federal Judicial Center, FEMA, First Data Systems, Fisher, Ford Aerospace, Ford Motor Company, Foxboro, Fraunhofer Institute, Gandalf Data, Gartner, GE FANUC Automation, General Dynamics, General Motors, General Services Administration, George Washington University, Global Technologies, Graphnet, Grumman, GTE, Harris, Hewlett-Packard, Honeywell, House Committee on Science, Howard University, Hughes, IBM, IBM-Canada, IBM-Italy, ICCC, ICE, ICL, ICOT, Illinois Bell, Incotel, Industrial Technology Institute, Infonet, Inner Consulting, Intel, Intelligence and Military Division, Inter Computer Comm., Interlan, Interop, Inc., IRS, Itautec, ITC/CMU, James Madison, Joint Tactical Command, Control and Communications Agency, JRM DND, Jupiter Technology, Korea Telecommunication Authority, Korea Telephone Company, Kwangson, Lantron, Lawrence Livermore Laboratory, Level-7 Ltd., Lincoln National Information Service, Linkware, Lockheed, Logica, Los Alamos, McDonnell-Douglas, Mandex, Martin Marietta, MCI, MICOM-I, Microtech, Mitech, Mitre Corporation, Modicon, Motorola, NARDAC, NASA, National Research Computer, Naval Data Services, Naval Oceanographic Office, Naval Research Laboratory, Naval Surface Warfare Center, NAVTASC, Navy, NBI, NCR Comten, NCSC, Netwise, Network Systems Corporation, NIST, Nixdorf, NMA-Northrop, NOAA, NOSC, Northern Telecom, Northrop, Novell, NSA, NTI, NYNEX, OAO Corporation, Oki Electric, Ltd., OMNICOM, Pacific Bell, Panadyne, Phillips Electronics, Ltd., Picture Elements, Planning Research Corporation, Prime Computers, Protocomm, Pyramid, Racal-Interlan, RADC/DCLD, Relational Technologies, Renex, Retix, Retix-Ireland, Rockwell, Science Applications, Semcor, Sequent Computers, Ship Star, Siemens, Silicon Graphics, Simpact Associates, Inc., SISCO, Soft-Switch, Southwest Bell, SPAG, Sprint International, SRA Corporation, SRI International, Stanford Telecommunications, Inc., Stanford University, Sterling Software, Stratus, Sun Microsystems, Swedish Institute of Technology, Swedish Telecom, Sydney, TASC, Tandem, Telecom, Telematica, Telenet, Texas Instruments, 3COM, TITN, Toshiba, Touch Communications, Transportation Services Institute, Trusted Information Systems, Inc., TRW, UK Department of Trade and Industry, UK Ministry of Defense, UMKC, Ungermann-Bass, Unified Technologies, Unisys Corporation, University of Delaware, University of Maryland, University of Michigan, University of Tennessee, University of Wisconsin-Madison, U.S. Air Force, USAISEC, U.S. Army, U.S. House of Representatives Information Systems, U.S. Senate, U.S. Systems, U.S. Treasury Department, U.S. West, Van Dyke, Verilin, Vitro Corporation, Wang Laboratories, Wellfleet, Western Union, Wollongong, Word Star, Xerox, Yankee Group, Yokogama

APPENDIX D

USERS' GUIDE EVALUATION FORM

The form contained herein contains a list of comments, questions and suggestions on this GOSIP Users' Guide. Readers of this Guide are encouraged to fill out this form and send it to the Chief, Systems and Network Architecture Division, Computer Systems Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899 (ATTN: GOSIP USERS' GUIDE COMMENTS). All comments received will be considered for future revisions of the GOSIP Users' Guide, and all comments are greatly appreciated.

GOSIP USERS' GUIDE
READER RESPONSE FORM

1. What did you like most about this Guide?

2. What did you like least about this Guide?

3. What information in this Guide did you find most helpful?

4. What specific suggestions do you have for improvements to this Guide?

NAME

ADDRESS

PHONE

REFERENCES

National Institute of Standards and Technology

1. NIST Special Publication 500-177, Stable Implementation Agreements for Open Systems Interconnection Protocols, Version 3. The successor to this document (NIST Special Publication 500-183) can be purchased from the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402. Stock Number 903-015-00000-4, Phone Order (202) 783-3238. This successor is also available from NTIS, phone order (703) 487-4650, and the IEEE Computer Society (1-800-272-6657).

2. Government Open Systems Interconnection Profile (GOSIP), Version 2, FIPS 146-1, October 1990, NTIS, Springfield, VA 22161.

3. Message Handling Systems Evaluation Guidelines, NIST SP 500-182.

4. POSIX FIPS 151-1, September 1990.

5. A Gateway Architecture Between SMTP and MHS, ICST-SNA-86-11.

6. A Gateway Architecture Between FTP and FTAM, ICST-SNA-86-6.

7. Trial of Open Systems Interconnection (OSI) Protocols Over Integrated Services Digital Network (ISDN), NIST IR 89-4160, August 1989.

8. GOSIP Conformance and Interoperation Testing and Registration, NISTIR 4594.

9. Message Handling Systems Interoperability Tests, NISTIR 4452.

10. FTAM Interoperability Tests, NISTIR 4435.

11. The U.S. GOSIP Testing Program, August 1990, NCSL/SNA-90/5.

International Organization for Standardization

1. Information Processing Systems - Open Systems Interconnection - Basic Reference Model, Ref. No. ISO 7498-1984(E)

2. Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management Part 1: General Introduction, ISO 8571/1, (ISO TC97/SC21 N2331).

3. Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management Part 2: The Virtual Filestore Definition, ISO 8571/2, (ISO TC97/SC21/N2332).

4. Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management Part 3: File Service Definition, ISO 8571/3, (ISO TC97/SC21/N2333).

5. Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management Part 4: File Protocol Specification, ISO 8571/4, (ISO TC97/SC21/N2334).

6. Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management Part 5: PICS Proforma, ISO 8571/5.

7. Information Processing Systems - Open Systems Interconnection - Virtual Terminal Service - Basic Class, IS 9040.

8. Information Processing Systems - Open Systems Interconnection - Vitrual Terminal Protocol - Basic Class, IS 9041.

9. Information Processing Systems - Local Area Networks- Part 3: Carrier Sense Multiple Access with Collision Detection, IS 8802/3.

10. Information Processing Systems - Local Area Networks - Part 4: Token Passing Bus Access Method and Physical Layer Specifications, IS 8802/4.

11. Information Processing Systems - Local Area Networks - Part 5: Token Ring Access Method and Physical layer Specifications, IS 8802/5.

12. Information Processing Systems - Open Systems Interconnection - Service Definition for Association Control Service Element: Association Control, ISO 8649, (ISO TC97/SC21/N2326).

13. Information Processing Systems - Open Systems Interconnection - Protocol Specification for Association Control Service Element: Association Control, ISO 8650, (ISO TC97/SC21/N2327).

14. Information Processing Systems - Open Systems Interconnection - Connection- Oriented Presentation Service Definition, ISO 8822, (ISO TC97/SC21/N2335).

15. Information Processing Systems - Open Systems Interconnection - Connection- Oriented Presentation Protocol Specification, ISO 8823, (ISO TC97/SC21/N2336).

16. Information Processing Systems - Open Systems Interconnection - Protocol for Providing the Connectionless Network Service, IS 8473, N3998, March 1986.

17. Information Processing Systems - Open Systems Interconnection - The Directory - Overview of Concepts, Models and Services, IS 9594, December 1988.

18. ISO 9542, End System to Intermediate System Routing Information Exchange Protocol for Use in Conjunction With the Protocol for the Provision of the Connectionless-Mode Network Service.

19. OSI Basic Reference Model - Part 2: Security Architecture. ISO/IS 7498-2

The above documents may be obtained from:

ANSI Sales Department
1430 Broadway
New York, NY 10018
(212) 642-4900

Consultative Committee for International Telegraph and Telephone

1. CCITT Recommendation X.25-1984, Interface Between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for Terminals Operating in the Packet Mode on Public Data Networks.

2. CCITT Recommendation X.400 (Red Book, 1984), Message Handling Systems: System Model-Service Elements.

3. CCITT Recommendation X.401 (Red Book, 1984), Message Handling Systems: Basic Service Elements and Optional User Facilities.

4. CCITT Recommendation X.408, (Red Book, 1984), Message Handling Systems: Encoded Information Type Conversion Rules.

5. CCITT Recommendation X.409 (Red Book, 1984), Message Handling Systems: Presentation Transfer Syntax and Notation.

6. CCITT Recommendation X.410, (Red Book, 1984), Message Handling Systems: Remote Operations and Reliable Transfer Server.

7. CCITT Recommendation X.411 (Red Book, 1984), Message Handling Systems: Message Transfer Layer.

8. CCITT Recommendation X.420 (Red Book, 1984), Message Handling Systems: Interpersonal Messaging User Agent Layer.

9. CCITT Recommendation X.430 (Red Book, 1984), Message Handling Systems: Access Protocol for Teletex Terminals.

10. CCITT Recommendation X.500, The Directory - Overview of Concepts, Models, and Services. December 1988.

11. CCITT Recommendation Q.921 (I.441) (Blue Book, 1988) ISDN User-Network Interface Data Link Layer Specification.

12. CCITT Recommendation Q.931 (I.451) (Blue Book, 1988) ISDN User-Network Interface Layer 3 Specification for Basic Call Control.

13. CCITT Recommendation X.31 (Blue Book, 1988) Support of Packet Mode Terminal Equipment by an ISDN.

The above documents may be obtained from:

International Telecommunications Union
Place des Nations
CH 1211
Geneve 20 SWITZERLAND

Miscellaneous

1. Manufacturing Automation Protocol, Version 3.0, July 1988, (plus supplement, May 1991), Corporation for Open Systems International, 1750 Old Meadow Road, McLean, VA 22102-4306 (ATTN: Customer Service).

2. Technical and Office Protocol, Version 3.0, August 1988, (plus supplement, May 1991), Corporation for Open Systems Inernational, 1750 Old Meadow Road, McLean, VA 22102-4306 (ATTN: Customer Service).

3. National Research Council. Executive Summary of the NRC Report on Transport Protocols for the Department of Defense Data Networks, RFC 939, February 1985.

4. MAP/TOP Position Paper on a Solution for Connection Oriented/Connectionless (CONS/CLNS) Network Services Interworking, November 16, 1987, Corporation for Open Systems International, 1750 Old Meadow Road, McLean, VA 22102-4306.

5. Eric Fleishmann and Bruce Hufless, November 9, 1990, "A Discussion of Token Ring Implementations," Network Architecture and Standards, Boeing Computer Services, Seattle, Washington.

6. U.S. GOSIP Registration Services, Instructions to Applicants, Draft Issue 1.1-1991, U.S. General Services Administration (GSA), Office of Telecommunications Services, 18th and F Streets, N.W., Washington, D.C. 20405

Department of Defense

1."Military Standard File Transfer Protocol," MIL-STD-1780, May 1984, Department of Defense, Washington, DC 20301.

2."Military Standard Simple Mail Transfer Protocol," May 1984, Department of Defense, Washington, DC 20301.

3. Memorandum, 2 July 1987, D.Latham, Subject: OSI Policy.

4. DOD OSI Implementation Strategy, May 1988, David Chappell, LCDR, Joint Tactical C3 Agency, Suite 210, 11440 Isaac Newton Square North, Reston, VA 22090-5006.

NIST-114A
(REV. 3-89)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

BIBLIOGRAPHIC DATA SHEET

1. PUBLICATION OR REPORT NUMBER
NIST/SP-500/192

2. PERFORMING ORGANIZATION REPORT NUMBER

3. PUBLICATION DATE
October 1991

4. TITLE AND SUBTITLE

Government Open Systems Interconnection Profile Users' Guide, Version 2

5. AUTHOR(S)
Tim Boland

6. PERFORMING ORGANIZATION (IF JOINT OR OTHER THAN NIST, SEE INSTRUCTIONS)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
GAITHERSBURG, MD 20899

7. CONTRACT/GRANT NUMBER

8. TYPE OF REPORT AND PERIOD COVERED
Final

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (STREET, CITY, STATE, ZIP)

Same as item #6

10. SUPPLEMENTARY NOTES

Supersedes NIST/SP-500/163

[ ] DOCUMENT DESCRIBES A COMPUTER PROGRAM; SF-185, FIPS SOFTWARE SUMMARY, IS ATTACHED.

11. ABSTRACT (A 200-WORD OR LESS FACTUAL SUMMARY OF MOST SIGNIFICANT INFORMATION. IF DOCUMENT INCLUDES A SIGNIFICANT BIBLIOGRAPHY OR LITERATURE SURVEY, MENTION IT HERE.)

This document assists Federal Agencies in planning for and procuring OSI. It provides tutorial information on OSI Protocols as well as information on OSI Registration, GOSIP Technical Evaluation, and GOSIP Transition Strategies.

12. KEY WORDS (6 TO 12 ENTRIES; ALPHABETICAL ORDER; CAPITALIZE ONLY PROPER NAMES; AND SEPARATE KEY WORDS BY SEMICOLONS)

Computer Networking, Data Communications, FTAM: GOSIP; Open Systems Interconnection, X.400

13. AVAILABILITY

[X] UNLIMITED

[ ] FOR OFFICIAL DISTRIBUTION. DO NOT RELEASE TO NATIONAL TECHNICAL INFORMATION SERVICE (NTIS).

[X] ORDER FROM SUPERINTENDENT OF DOCUMENTS, U.S. GOVERNMENT PRINTING OFFICE, WASHINGTON, DC 20402.

[X] ORDER FROM NATIONAL TECHNICAL INFORMATION SERVICE (NTIS), SPRINGFIELD, VA 22161.

14. NUMBER OF PRINTED PAGES
166

15. PRICE

ELECTRONIC FORM

☆U.S. GOVERNMENT PRINTING OFFICE:1991 -311 -944/62626

ANNOUNCEMENT OF NEW PUBLICATIONS ON COMPUTER SYSTEMS TECHNOLOGY

Superintendent of Documents
Government Printing Office
Washington, DC 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued in the series: National Institute of Standards and Technology Special Publication 500-.

Name _____

Company _____

Address _____

City _____ State _____ Zip Code _____

(Notification key N-503)

NIST Technical Publications

Periodical

Journal of Research of the National Institute of Standards and Technology—Reports NIST research and development in those disciplines of the physical and engineering sciences in which the Institute is active. These include physics, chemistry, engineering, mathematics, and computer sciences.
Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Institute's technical and scientific programs. Issued six times a year.

Nonperiodicals

Monographs—Major contributions to the technical literature on various subjects related to the Institute's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NIST, NIST annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NIST under the authority of the National Standard Data Act (Public Law 90-396). NOTE: The Journal of Physical and Chemical Reference Data (JPCRD) is published bi-monthly for NIST by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements are available from ACS, 1155 Sixteenth St., NW., Washington, DC 20056.

Building Science Series—Disseminates technical information developed at the Institute on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NIST under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NIST administers this program as a supplement to the activities of the private sector standardizing organizations.

Consumer Information Series—Practical information, based on NIST research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.
Order the **above** *NIST publications from: Superintendent of Documents, Government Printing Office, Washington, DC 20402.*
Order the **following** *NIST publications—FIPS and NISTIRs—from the National Technical Information Service, Springfield, VA 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NIST pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NIST Interagency Reports (NISTIR)—A special series of interim or final reports on work performed by NIST for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service, Springfield, VA 22161, in paper copy or microfiche form.

U.S. Department of Commerce
National Institute of Standards and Technology
Gaithersburg, MD 20899

Official Business
Penalty for Private Use $300