U. S. Government Open Systems Interconnection Profile (GOSIP)

VERSION 2.0

October 1990

TABLE OF CONTENTS

APPENDICES

LIST OF FIGURES

LIST OF TABLES

FOREWORD

The U.S. Government Open Systems Interconnection (OSI) Advanced Requirements Group was established by the National Institute of Standards and Technology (NIST) in cooperation with the Information Resource Managers of the Federal agencies. The group's purpose is to coordinate the acquisition and operation of OSI products by the Federal government. This document specifies the U. S. Government OSI profile. A profile is a cross-section of functional applications pertaining to a particular environment.

It is expected that the Administrator of the General Services Administration (GSA) will provide for the implementation of Open Systems Interconnection (OSI) according to this profile.

The National Institute of Standards and Technology (NIST) will issue this profile as a Federal Information Processing Standard (FIPS). This is Version 2 of the Government Open Systems Interconnection Profile. It contains an updated specification of the OSI protocols that meet government needs. Products based on these protocols are or soon will be available from major vendors.

Organizations contributing to the development of this profile are given below.

Department of Agriculture
Department of Commerce
Department of Defense
Department of Energy
Department of Education
Department of Health and Human Services
Department of Housing and Urban Development
Department of the Interior
Department of Justice
Department of Labor
Department of Transportation
Department of the Treasury
Environmental Protection Agency
General Services Administration
Library of Congress
National Aeronautics and Space Administration
National Communications System
National Science Foundation
Office of Management and Budget
Veterans Administration

PREFACE

This is a Federal Government procurement profile for open systems computer network products. Section 1 contains introductory material, the purpose and scope of the profile, and the sources of the protocol specifications contained in the profile. Section 2 contains general statements on conformance, interoperation and performance of network systems covered by this profile. Section 3 contains a brief description of the OSI architecture and protocols that apply to this profile. The network protocols are specified in section 4, the principal part of this profile. Accompanying each protocol implementation reference is a statement of conformance identifying the required functional units of that protocol. section 5, Addressing Requirements, is also an integral and mandatory part of this profile. Technical Support Personnel to Acquisition Authorities must be familiar with the terminology and ideas expressed in sections 4 and 5.

Section 6 defines security options that, if needed, must be explicitly requested in Requests For Proposals.

This profile will change with improvements in technology and with the evolution of network protocol standards. Appendices specify future work items needed to enrich the profile, and thus, improve its utility to the agencies.

GLOSSARY

The terms defined below are used frequently throughout this profile. They are defined here to aid the lay reader. Other terms appearing in sections 4 and 5 are defined in Federal Standard 1037A and ISO 7498 and must be thoroughly understood by the Technical Support Personnel to Acquisition Authorities.

Protocol

In the Open Systems Interconnection reference model, the communication functions are partitioned into seven layers. Each layer, N, provides a service to the layer above, N+1, by carrying on a conversation with layer N on another processor. The rules and conventions of that N-layer conversation are called a protocol.

End System

An end system (ES) contains the application processes that are the ultimate sources and destinations of user oriented message flows. The functions of an end system can be distributed among more than one processor/computer.

Intermediate System

An intermediate system (IS) interconnects two or more subnetworks. For example, it might connect a local area network with a wide area network. It performs routing and relaying of traffic. A processor can implement the functions of both an end system and an intermediate system.

A system implementing all seven layers of protocol may provide service directly to users (acting as an end system), and it may connect subnetworks (acting as an intermediate system). When it performs the functions of an intermediate system, only the lower three layers of protocol are exercised.

Open System

An open system is a system capable of communicating with other open systems by virtue of implementing common international standard protocols. End systems and intermediate systems are open systems. However, an open system may not be accessible by all other open systems. This isolation may be provided by physical separation or by technical capabilities based upon computer and communications security.

Federal Government Terminology

The following definitions are informal and generic and are provided for the benefit of private sector organizations that review the profile. Agency regulations and any contract should be referred to for precise terms and their usage. Also, other terms may be used in lieu of these in agency regulations and in specific contracts.

Acquisition Authority

An Acquisition Authority, commonly known as a contracting officer, is an individual who, under Federal law and acquisition regulations, has the authority to enter into, administer, and/or terminate a government contract.

Federal Acquisition Regulation (FAR)

The FAR is applicable to Executive departments and agencies of the Federal Government in the area of acquisition, leasing, and rental of personal property and services. Many departments and agencies have supplementary regulations that apply to their acquisitions.

Federal Information Resources Management Regulation (FIRMR)

The FIRMR is applicable to federal departments and agencies in the areas of management, acquisition and use of information resources, including automatic data processing and telecommunications equipment and services.

Requests For Proposals (RFP)

Requests For Proposals are documents issued by the government to request bids for products or services.

1. INTRODUCTION

1.1 BACKGROUND

Both the government and the private sector recognize the need to develop a set of common data communication protocols based on the International Organization for Standardization's seven-layer Open Systems Interconnection (OSI) Basic Reference Model [ISO 1]. In the past, vendor-specific implementations of data communication protocols led to isolated domains of information, very difficult and expensive to bridge. Recent advances in communication technology based on the OSI model offer alternatives to vendor-specific network solutions. Most significantly, advances in open systems allow the interoperation of end systems of different manufacture, when required.

This Government Open Systems Interconnection Profile (GOSIP) is based on agreements reached at the National Institute of Standards and Technology (NIST) Workshop for Implementors of Open Systems Interconnection. Each new version of GOSIP will reference the latest appropriate version of the Stable Implementation Agreements for Open Systems Interconnection Protocols [NIST 1], hereafter referred to as the Workshop Agreements. The Workshop Agreements record stable implementation agreements of OSI protocols among the organizations participating in the NIST Workshop for Implementors of OSI.

A new version of the Workshop Agreements is created each year at the December OSI Implementors' Workshop meeting. It is the intent of the NIST Workshop that new versions of the Workshop Agreements will be backwardly compatible with previous versions. New editions of the same version of the Workshop Agreements are published at regular intervals during the year. These new editions contain errata and clarifications to the original agreements that are approved by the Workshop plenary. The latest editions are being distributed to all workshop attendees and are available through the National Technical Information Service (NTIS). See NIST Reference 1 for ordering information.

GOSIP is also consistent with and complementary to industry's Manufacturing Automation Protocol (MAP) [MISC 1] and Technical and Office Protocols (TOP) [MISC 2] specifications. GOSIP addresses the need of the Federal Government to move immediately to multi-vendor interconnectivity without sacrificing essential functionality already implemented in critical networking systems. All capabilities described herein exist as standard products or are close enough to market that they can be proposed by vendors.

1.2 PURPOSE

This profile is the standard reference for all federal government agencies to use when acquiring and operating ADP systems or services and communication systems or services intended to conform to ISO Open Systems Interconnection protocols which provide interoperability in a heterogeneous environment.

1.3 EVOLUTION OF THE GOSIP

The GOSIP FIPS will be 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 will supersede the previous version of the document because it will include all of the protocols in the previous version plus additional new protocols. Procurement of the new protocols is mandated in Federal procurement requests initiated eighteen months after the version of GOSIP containing those protocols is promulgated as a FIPS. Every new version of GOSIP will specify 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 protocol.

It is a goal that a new version of GOSIP will be upwardly 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 will be identified in the new GOSIP version. Unless otherwise stated, the mandatory compliance date of the previous version of GOSIP also

applies to the errata. These errata will not be 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. See section 1.7 for the GOSIP Version 1 errata.

1.4 SCOPE

In an increasingly complex world, the need to exchange information has become an ever more important factor in conducting business. Federal agencies need to share information not only with other Federal agencies, but with state and local governments and commercial organizations as well. Until recently, computer networking technology has not kept pace with this need to communicate. Even now, many Federal agencies have "islands" of computer systems built by different vendors, or by the same vendor, that cannot interoperate.

The GOSIP, in addition to being a Federal mandate, is an alert that the vendor community has developed a nonproprietary solution for this requirement to exchange information. The solution is the OSI protocols upon which GOSIP is based. Version 1 of GOSIP (FIPS 146) provided electronic mail and file transfer services using the OSI standards for Message Handling Systems (MHS) and File Transfer, Access, and Management (FTAM). Version 1 of GOSIP provided interoperability among users on X.25, 802.3, 802.4, and 802.5 subnetworks. In addition, Version 1 of GOSIP created a foundation upon which to build new protocols providing new services useful to Federal agencies.

Version 2 of GOSIP (FIPS 146-1) uses that foundation to provide a remote terminal access capability using the Virtual Terminal (VT) standard. At the network layer, Version 2 of GOSIP extends interoperabity to include ISDN subnetworks. Future versions of GOSIP will add new user services such as Directory Services, Transaction Processing, Electronic Data Interchange and Remote Data Base Access as well as allow interoperability among users served by other network technologies.

GOSIP does not mandate that government agencies abandon their favorite computer networking products. GOSIP does mandate that government agencies, when acquiring computer networking products, purchase OSI capabilities in addition to any other requirements, so that multi-vendor interoperability becomes a built-in feature of the government computing environment, a fact of life in conducting government business.

The OSI protocols have the potential to change the way the Federal Government does business. It is essential that Federal agencies make a strategic investment in OSI beginning now, so that they will be well positioned to take advantage of the new services provided by the OSI protocols as they become available. Planning the integration of OSI may require considerable time and effort, but this work will be more than offset by the benefits provided by the new technology.

1.5 APPLICABILITY

GOSIP specifies a set of OSI protocols for computer networking that is intended for acquisition and use by government agencies. It must be used by all Federal government agencies when acquiring products and services which provide equivalent functionality to the OSI protocols referenced in this document. For a more detailed statement of applicability, see FIPS 146.

1.6 GOSIP VERSION 2 FUNCTIONALITY

Version 2 of GOSIP contains the following functionality not included in Version 1.

1. The Virtual Terminal Service (TELNET and Forms profiles);
2. The Office Document Architecture (ODA);
3. The Integrated Services Digital Network (ISDN);
4. The End System-Intermediate System protocol (ES-IS), and as user options;
5. The Connectionless Transport Service (CLTS); and,
6. The Connection-Oriented Network Service (CONS).

The compliance information for GOSIP Version 2 functions is stated in the FIPS announcement. Since the Connectionless Transport Service and the Connection-Oriented Network Service are provided as optional user services, there is no mandatory compliance specified. All GOSIP protocols not included in the above list are bound by the GOSIP Version 1 compliance date which is August 15, 1990. Figure 3.1 illustrates the GOSIP Version 1 architecture and protocols. Figure 3.2 illustrates the GOSIP Version 2 architecture and protocols.

1.7 GOSIP Version 1 Errata

1. Since Version 1 of the Stable Implementation Agreements for OSI Protocols was published, errata have been added to those agreements, primarily by the FTAM and Upper Layer Special Interest Groups (SIGs) of the NIST OSI Implementors' Workshop to correct problems in the original agreements and to align with agreements being developed internationally. Version 1 of GOSIP will now reference the relevant sections of Version 3 of the Stable Implementation Agreements. Text for these sections is available from the Government Printing Office and NTIS.

2. Version 1 of GOSIP (section 5.3.2) required that private messaging systems within the government be capable of routing on administration name, private domain name, organization name, organization unit and personal name. The requirement that private messaging systems be capable of routing based on personal name has been deleted. This change expands the range of messaging systems that are GOSIP compliant.

3. GOSIP Version 1 implementations should use the Network Service Access Point (NSAP) Address structure in Figure 5.1.3 of GOSIP Version 2. This change was made to align with the routing standards currently being developed by the ISO.

4. Version 1 of GOSIP (section 4.2.3) required that processing of Protocol Data Units by the Connectionless Network Layer Protocol be in order of priority. This requirement has been deleted.

5. Version 1 of GOSIP describes a general architecture for OSI security, defines a set of optional security services that may be supported within the OSI model, and outlines a number of mechanisms that can be used in providing the service. Users should now refer to the updated Security Options section in Version 2 of GOSIP. It should be noted that, even in Version 2 of GOSIP, the security section is optional and is considered a placeholder for future security specifications.

1.8 SOURCES OF PROTOCOL SPECIFICATIONS

1.8.1 Primary Source

The primary source of protocol specifications in GOSIP is the Stable Implementation Agreements for Open Systems Interconnection Protocols [NIST 1]. This source document was created and is maintained by the NIST Workshop for Implementors of Open Systems Interconnection. It provides implementation specifications that are derived from service and protocol standards issued by the International Organization for Standardization (ISO), the Consultative Committee for International Telegraphy and Telephony (CCITT), and the Institute of Electrical and Electronics Engineers, Inc. (IEEE).

By primary source, it is meant that where GOSIP uses a given protocol, it cites that protocol by reference as specified in the above-named Workshop Agreements. The primary source is used in all instances where the protocol of interest has been specified in the Workshop Agreements. Section 4 of this profile gives conformance statements for each protocol that, in some cases, are augmented from the minimal conformance statements in the Workshop Agreements in order to provide the functionality required for government computer networking.

1.8.2 Secondary Sources

GOSIP must be complete in that open systems procured in accordance with it must interoperate and must provide service generally useful for government computer networking applications. The Workshop Agreements continue to evolve, but they are still incomplete. (The appendices of GOSIP cite needed work.) Thus, where the Workshop Agreements do not provide completeness, GOSIP may augment protocol and service specifications from the following sources, listed in precedence order.

- International Standards and Recommendations
- Draft International Standards

Since this profile is one of open systems, the secondary sources include specifications that are international standards or are advancing to become international standards. They are included in GOSIP, where needed, to help satisfy the criterion of completeness, and thus, utility. Note that secondary sources exclude protocols, however mature, that are not a part of the international standards process.

1.8.3 Tertiary Sources

Even the secondary sources named above may not provide a complete and useful networking system today. It may be necessary for GOSIP to augment protocol and service specifications from the following sources, listed in precedence order.

- ANSI Standards
- Draft Proposed International Standards
- Federal Information Processing Standards
- Military Standards

For example, security protocols might be incorporated from a FIPS issued by NIST. The use of protocols from other than the primary and secondary sources is undesirable. It is expressly intended that these omissions from standards work be brought to the attention of the international standards bodies so that acceptable international standards may be developed as rapidly as possible. The GOSIP Advanced Requirements Group will replace all tertiary source protocols in GOSIP with suitable primary and secondary source substitutes, when available.

2. TESTING OF GOSIP-COMPLIANT PRODUCTS

Conformance testing verifies that an implementation acts in accordance with a particular specification, such as GOSIP. Interoperability testing duplicates the "real-life" environment in which an implementation will be used. Performance testing measures whether an implementation satisfies the performance criteria of the user. Functional testing determines the extent to which an implementation meets user functional requirements.

NIST issued GOSIP Version 1.0 testing guidance in GOSIP Conformance and Interoperation Testing and Registration [NIST 8]. Consult that reference for detailed procedures, instructions for GOSIP product suppliers, and recommendations for Acquisition Authorities. 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 2.0. Until such revision occurs, Federal agency personnel should use, for testing GOSIP Version 2.0 additions, the interim guidance supplied below in sections 2.1 and 2.2.

NIST issued Message Handling Systems Evaluation Guidelines [NIST 9] to assist Federal agency personnel to evaluate the degree to which specific Message Handling Systems products meet the specific performance and functional requirements of an agency procurement. Further guidelines are planned; File Transfer, Access and Management will be the next. If a guideline is not yet available for an application of interest, Federal agency personnel should use the interim guidance supplied in sections 2.3, 2.4, and 2.5.

2.1 CONFORMANCE TESTING

Conformance is shown by the vendor having passed conformance tests adequate for the purpose of exercising the functional units specified in section 4. Conformance to the GOSIP will only apply to the profile defined by the Acquisition Authority. For the purposes of testing conformance to the protocols required by GOSIP Version 2.0, the Acquisition Authority will provide documentation which identifies specific testing requirements.

Conformance tests and test systems are currently being developed by several testing organizations. When these test systems for GOSIP Version 2.0 are completed, NIST will specify the tests, test systems and testing organizations that are accredited to perform conformance testing of GOSIP protocols.

For the interim, the Acquisition Authority shall require that vendors substantiate any claim of GOSIP conformance.

The Acquisition Authority shall also be responsible for determining that acceptable test results are available as a prerequisite to awarding of a final procurement contract.

2.2 INTEROPERABILITY TESTING

The Acquisition Authority should specify a detailed set of requirements that will serve to test interoperability of GOSIP Version 2.0 protocols. The Acquisition Authority must specify the following for this testing:

- the products to be used for the interoperability testing, including hardware and software versions and components,

- a detailed description of planned test scenarios to be run between implementations in the interoperability testing, including the results expected, and

- criteria for passing or failing the testing.

NIST will recommend vehicles particularly suitable for interoperability testing.

2.3 PERFORMANCE TESTING

The principal thrust of OSI is to provide interworking of distributed applications using heterogeneous, multi-vendor systems. GOSIP does not cite performance criteria. Note that protocol definitions include quality of service parameters and other tunable functions. The Acquisition Authority must determine and specify those performance related features that are desired to be under user or application process control and those desired to be under system operator control. The Acquisition Authority may also wish to specify benchmarking criteria as evidence of satisfying performance requirements.

2.4 FUNCTIONAL TESTING

The GOSIP specification mandates for each protocol a minimum set of functions to meet general government requirements. In many instances additional functions might be supported within the Workshop Agreements and/or the protocol standard. The Acquisition Authority must determine and specify such additional functions that are required within an acquisition. The Acquisition Authority is responsible for determining that the vendor products proposed meet any and all functional requirements.

2.5 VENDOR ENHANCEMENTS

It is expected that most vendors will update their products, for example, from a Draft International Standard version to an International Standard version, as implementation specifications are completed in the Workshop Agreements. Also, some vendors may provide additional functionality. Implementations that go beyond the functional units stated in section 4 must be implemented according to the Workshop Agreements and must interwork with implementations that strictly comply with section 4. Requests For Proposals should encourage vendor enhancements where required to meet user needs.

3. DESCRIPTIONS OF ARCHITECTURE AND PROTOCOLS

This section briefly describes the GOSIP architecture and protocols. For a more thorough understanding, consult the Government Open Systems Interconnection User's Guide [NIST 7] and other references cited in this profile.

3.1 ARCHITECTURE DESCRIPTION

Figure 3.1 illustrates the GOSIP Version 1 architecture and protocols. Figure 3.2 shows how new protocols providing new services have been added to GOSIP Version 2 while maintaining compatibility with GOSIP Version 1.

Achieving OSI within the government is best accomplished by using a single method (one protocol profile at each OSI layer) to perform the functions of routing and reliable data transfer. Fig. 3.2 shows that these functions are provided by the transport class 4, and connectionless network layer protocols. Mandatory use of a single transport protocol class (class 4) and a connectionless network layer protocol (CLNP) assures interoperable data transfer between government computer systems for a variety of applications across a variety of subnetwork technologies. Optional use of additional transport and network layer protocols is not precluded by GOSIP; in fact, as shown in Figure 3.2, GOSIP now includes specifications for an optional connectionless transport service and an optional connection-oriented network service. The specifications give sufficient detail for achieving interworking among government computer systems implementing these options.

It is useful to enable user selection from among a set of lower layer subnetwork technologies for local and wide area networking. These different technologies exhibit physical, performance, and cost differences that render one technology more appropriate than others for particular uses. Fig. 3.2 illustrates six subnetwork technologies specified by GOSIP. These are the packet data network (X.25), the point to point (Pt-Pt) LAP B Subnetwork, the Integrated Services Digital Network (ISDN), the Token Bus (ISO 8802/4), the Token Ring (ISO 8802/5) and the Carrier Sense Multiple Access with Collision Detection (ISO 8802/3). When a point to point or local area subnetwork technology is selected, the CLNP end system to intermediate system (CLNP ES-IS) routing protocol [ISO 44] is also required. Other lower layer subnetwork technologies may be used, but the Acquisition Authority must provide proper specification to ensure procurement of an effective product, that is, a product able to support operation of transport class 4, the connectionless network protocol, and the GOSIP upper layer protocols.

Interconnection of multiple wide-area networks to form the appearance of a single logical wide-area network may be accomplished by any technically appropriate means such as X.75 gateways. Interconnection of remote local area networks to form the appearance of a single logical network may be accomplished by any technically appropriate means, such as MAC bridges. In all other instances, the GOSIP mandates subnetwork interconnection by means of the CLNP and the network access methods appropriate for the specific networks being interconnected.

At the application layer, many protocols are expected to be included in GOSIP over time, each applying to different uses. In Fig. 3.2, the current application protocols are File Transfer, Access and Management (FTAM) based on the ISO International Standard [ISO 16-19], the Basic Class Virtual Terminal Protocol based on the ISO International Standard [ISO 32-35], and Message Handling Systems based on the 1984 CCITT Recommendations [CCITT 2-9]. Each application may require a different selected set of services from the application control service elements and the presentation and session control layers. Thus, layers 5, 6, and 7 may be thought of as an integral package of GOSIP upper layer protocols for each specific application.

Figure 3.1 GOSIP Version 1 OSI Architecture

Figure 3.2 GOSIP Version 2 OSI Architecture

The Office Document Architecture (ODA) standard based on the ISO International Standards [ISO 36-42, CCITT 17-24] is also included in GOSIP. Although ODA is not an OSI protocol, it is included in GOSIP because it provides services required by Federal agencies, and the information specified by the standards can be transported by the OSI FTAM and MHS Application layer protocols.

A goal of this profile is to permit an Acquisition Authority to issue unambiguous procurement requests for standard applications operating over networks using standard protocols. The Acquisition Authority determines the required applications and the required networks and the GOSIP defines the required protocols. For example, if an Acquisition Authority requires a general purpose File Transfer Access and Management application on a CSMA/CD subnetwork, the GOSIP defines that layer 7 FTAM is required along with certain services from the application control service elements, presentation, and session protocols. To perform the data transfer function, GOSIP mandates the Class 4 transport protocol and the connectionless network layer protocol, and defines a subset of the ISO 8802/2 link layer, and the ISO 8802/3 CSMA/CD protocol.

3.2 PROTOCOL DESCRIPTIONS

Following are brief narratives of the general services provided by protocols in each layer of the GOSIP architecture to the layer above.

The Application layer (layer 7) allows for protocols and services required by particular user-designed application processes. Functions satisfying particular user requirements are contained in this layer. Representation and transfer of information necessary to communicate between applications are the responsibility of the lower layers. See References [NIST 1; ISO 1, 16-19, 22-25, 32-35; CCITT 2-9, 14].

The Presentation layer (layer 6) specifies or, optionally, negotiates the way information is represented for exchange by application entities. The presentation layer provides the representation of: 1) data transferred between application entities, 2) the data structure that the application entities use, and 3) operations on the data's structure. The presentation layer is concerned only with the syntax of the transferred data. The data's meaning is known only to the application entities, and not to the presentation layer. See References [NIST 1; ISO 1,20,21,24,25].

The Session layer (layer 5) allows cooperating application entities to organize and synchronize conversation and to manage data exchange. To transfer the data, session connections use transport connections. During a session, session services are used by application entities to regulate dialogue by ensuring an orderly message exchange on the session connection. See References [NIST 1; ISO 1,14,15; CCITT 12,13].

The Transport layer (layer 4) connection-oriented service provides reliable, transparent transfer of data between cooperating session entities. The transport layer entities optimize the available network services to provide the performance required by each session entity. Optimization is constrained by the overall demands of concurrent session entities and by the quality and capacity of the network services available to the transport layer entities. In the connection-oriented transport service, transport connections have end-to-end significance, where the ends are defined as corresponding session entities in communicating end systems. Connection-oriented transport protocols regulate flow, detect and correct errors, and multiplex data, on an end-to-end basis. See References [NIST 1; ISO 1,12,13; CCITT 10,11]. The transport layer also supports a simple connectionless transport service [ISO 46-47].

The Network layer (layer 3) provides message routing and relaying between end systems on the same network or on interconnected networks, independent of the transport protocol used. The network layer may also provide hop-by-hop network service enhancements, flow control, and load leveling. Services provided by the network layer are independent of the distance separating interconnected networks. See References [NIST 1,3; ISO 1-8,11; CCITT 1; NCS 1].

The Data link layer (layer 2) provides communication between two or more (multicast service) adjacent systems. The data link layer performs frame formatting, error checking, addressing, and other functions necessary to ensure accurate data transmission between adjacent systems. Note that the data link layer can operate in conjunction with several different access methods in the physical layer. See Figure 3.2 for examples. See References [NIST 1-3,5; ISO 1,26,28; CCITT 1].

The Physical layer (layer 1) provides a physical connection for transmission of data between data link entities. Physical layer entities perform electrical encoding and decoding of the data for transmission over a medium and regulate access to the physical network. See References [NIST 1-3; ISO 1; ISO 29-31; IEEE 1].

4. PROTOCOL SPECIFICATIONS

4.1 USE OF THE LAYERED PROTOCOL SPECIFICATIONS

The individual protocol and interface specifications in this section shall be used directly in Requests For Proposals. However, Acquisition Authorities must take additional steps to ensure an adequate specification for their intended purpose. The following items must be supplied by the Acquisition Authority.

4.1.1 Protocol Selection

The architecture described in section 3 suggests a range of protocol choices at different layers of the OSI Reference Model. A subset of these protocols may adequately satisfy an individual acquisition requirement, and may be used. If a subset of the protocols and interface profiles is chosen, it is the Acquisition Authority's responsibility to ensure that all paths through the architecture are complete, i.e., (1) that protocols from layer 1 through layer 7 are included for end systems and at least layers 1 through 3 are included for intermediate systems, and (2) that the appropriate service interface specifications for the selected protocols are also included, as indicated in section 4.1.2 below.

With respect to selecting protocols, at least one lower layer technology must be chosen, i.e., CSMA/CD (carrier sense, multiple access with collision detection) [NIST 1, 2; ISO 28, 29], Token Bus [NIST 1; ISO 28, 30], Token Ring [NIST 1; ISO 28, 31]; X.25 [NIST 1, 3; CCITT 1; ISO 8]; HDLC LAP B point to point (Pt-Pt) subnetwork [ISO 26] or ISDN [NIST 1, ANSI 1-3, CCITT 25-27, ISO 45]. Additional lower layer technologies may be used to meet special requirements. The following protocol layers are mandatory for compliance with GOSIP: the connectionless network layer protocol, transport class 4, and session. Transport class 0 and the Connection Oriented Network Service (CONS) [ISO 2,3] are mandated only in conjunction with public data network messaging; see section 4.2.7.3, Message Handling Systems. Presentation protocol and association control service elements are required for all applications except messaging. At least one application layer specific protocol is required to support the intended application. For example, if messaging is required, specify MHS; if file transfer is required, specify FTAM; and, if the Virtual Terminal Service is required, specify VT. The provision of the CONS, for general use, and the Connectionless Transport Protocol (CLTP) are options that may be specified in addition to the GOSIP mandatory Connectionless Network Service (CLNS) and Transport (class 4), respectively. More detailed specification guidance is provided in sections 4.2 and 4.3.

4.1.2 Service Interface Requirements

GOSIP mandates no service interface accessibility beyond that indicated in the Workshop Agreements; therefore, any additional service interface accessibility requirements must be clearly stated and mandated by the Acquisition Authority. For example, GOSIP mandates no specific direct access to transport services. If the Acquisition Authority requires direct access to transport services, such a requirement must be included in a solicitation. The issues involved in determining such a requirement are complex. Refer to the GOSIP Users' Guide for a discussion of these issues.

Should the Acquisition Authority not request direct access to service interfaces, such access might or might not be provided at the discretion of individual vendors. For example, some vendors may provide access to session services, others may provide access to transport and network services, and still others may limit access to association control services only. Of course, some vendors may provide direct access to service interfaces at the human user interface only. When there is no requirement for a service interface between layers, vendors might merge multiple layer implementations. Such a merger is often implemented to accrue performance benefits to the user.

Should the Acquisition Authority request direct access to a specific service interface, care should be taken to specify the general functional and operational objectives of the interface; otherwise, particular vendor interface implementations might or might not meet user requirements. While specifying the general functional and operational objectives for a service interface should enable the vendor to meet a user's functional requirements, such a specification will not ensure portability of software, written to the interface, across product lines from multiple vendors. Work underway in the IEEE 1003.8 POSIX networking services interface committee should create, in the future, a series of service interface specifications that will enable portability of software written to those specifications. In the interim, Acquisition Authorities requiring service interfaces that enable software portability must include a very detailed and explicit interface specification within the solicitation. Such a specification is difficult and expensive to produce, and will limit the number of vendors that bid on a solicitation. Thus, this practice is not recommended. A more prudent course, at the present time, is to specify the general functional and operational objectives of a service interface, leaving implementation decisions to the vendor.

4.1.3 Performance Requirements

The Acquisition Authority must specify performance requirements. Performance of an open system is a function of: 1) the source end system, 2) the destination end system, and 3) the communications links, subnetworks, and intermediate systems between the two end systems. The Acquisition Authority's best strategy, given these difficult-to-control factors, is to specify performance requirements for the principal operating environment of the end system. For example, if the communicating end systems will generally be on the same token bus network, detailed performance profiles should be developed for that environment. If these systems must occasionally communicate over a packet data network between local area networks (LANs), then a test for correct interoperation in this occasional environment, without strict performance requirements, should also be included.

4.2 END SYSTEM SPECIFICATION

4.2.1 Physical Layer

GOSIP does not mandate any specific physical interface standard. However, the Acquisition Authority must specify physical layer requirements in a solicitation. The following interfaces are recommended. The three standards most commonly used in conjunction with X.25 are Electronic Industries Association (EIA) RS-232-C [EIA 1] for line speeds up to 19.2 kilobits/second, V.35 [CCITT 16] for line speeds above 19.2 kilobits/second, and EIA RS-530 for transfer rates above 20 kilobits/second. For IEEE 802 LANs, the physical interface characteristics are identified in ISO 8802/3 for CSMA/CD, ISO 8802/4 for token bus, and ISO 8802/5 for token ring, [ISO 29-31]. Additional specifications for these interfaces, including subsets, options, and parameter settings are included in the Workshop Agreements [NIST 1]. For ISDN, GOSIP provides for the basic rate interface (BRI) at the S, T, and U reference points [ANSI 1-2] and the primary rate interface (PRI) at the U reference point [ANSI 3]. The BRI provides a 16 kilobits/second signalling (D) channel and up to two 64 kilobits/second switched (B) channels. The PRI provides a 64 kilobits/second signalling (D) channel and up to twenty-three 64 kilobits/second switched (B) channels.

Other, non-proprietary, physical interface standards may be selected depending upon unique requirements of the Acquisition Authority; however, the Acquisition Authority must take special care to ensure appropriate operation of such interfaces within a procured system. The Acquisition Authority is advised to make a selection from the set of recommended physical interfaces.

4.2.2 Data Link Layer

The data link layer protocols shall be selected by the Acquisition Authority from among the following: 1) High Level Data Link Control (HDLC) Link Access Procedure B (LAP B), in conjunction with X.25 [NIST 1,3; ISO 26] and Pt-Pt subnetworks; 2) ISO 8802/2 (LLC 1) in conjunction with ISO 8802/3, ISO 8802/4, or ISO 8802/5 [NIST 1; ISO 28], and 3) Q.921 (LAPD) [CCITT 25] for operation on the ISDN D channel and ISO 7776 (LAP B) for operation on ISDN B channels. These protocols shall conform to the Workshop Agreements.

4.2.3 Network Layer Service

For GOSIP end systems, the connectionless network service (CLNS) is mandated for Government-wide interoperability and provides the required means of interconnecting logically distinct local and long-haul subnetworks. When a GOSIP end system is connected to a local area or Pt-Pt subnetwork, the CLNP end system to intermediate system (CLNP ES-IS) dynamic routing protocol is required. The connection-oriented network service is an option available to GOSIP end systems directly connected to an X.25 subnetwork or ISDN. The technology for providing X.25 and ISDN subnetworks may be used to support the mandated CLNS and the optional CONS; in either case certain subnetwork access protocols are required. These topics are elaborated in the following paragraphs.

4.2.3.1 Connectionless Mode Network Service

The Connectionless Mode Network Service (CLNS) shall be provided by the ISO Connectionless Network Protocol (CLNP) [NIST 1; ISO 4,7]. The CLNP must be implemented and used for internetworking of concatenated subnetworks. For operation on a single logical subnetwork, the CLNP also must be implemented. When an end system is connected to a local area or Pt-Pt subnetwork the CLNP ES-IS protocol must be implemented and used.

4.2.3.1.1 Provision of the Connectionless Network Service

This service shall be provided according to the Workshop Agreements, section 3.5, with the following modifications and additions:

Add to the first bullet of section 3.5.1(2), the following:

- o An End System must provide a configuration mechanism to control the value to be assigned to the Lifetime parameter for PDUs which it originates.

Replace the first bullet of section 3.5.1(3) Optional Functions with the following:

- o The use of the security parameter shall be in accordance with section 6 of this specification, if required by the Acquisition Authority.

Add as section 3.5.2(4):

- o The CLNS shall be provided with interfaces to the 1984 CCITT Recommendation X.25, HDLC LAP B (ISO 7776), ISO 8802.2 and Draft International Standard (DIS) 9574 (ISDN), as selected by the Acquisition Authority. When interface to DIS 9574 is provided, the provisions of ISO 8878 are not used.

Section 3.5.3 of the Workshop Agreements is to be implemented by those systems operating over

X.25. Section 3.5.4 of the Workshop Agreements is to be implemented by those systems operating over ISDN.

4.2.3.1.2 Provision of The End System To Intermediate System Routing Service

For end systems connected to local area and Pt-Pt subnetworks, the end system to intermediate system (CLNP ES-IS) routing service shall be provided by the ES-IS protocol ISO 9542 [ISO 44] implemented as specified in the Workshop Agreements section 3.8.1. For end systems connected to wide-area networks, provision of an end system to intermediate system routing service is network specific.

4.2.3.2 Connection-Oriented Network Service

The CONS is an additional, optional service that may be specified for end systems that are directly connected to X.25 wide area networks and ISDNs. Use of this service can, under certain circumstances, avoid the overhead associated with CLNP and may permit interoperation with end systems that do not comply with GOSIP (i.e., do not implement CLNP). When an Acquisition Authority specifies the CONS option, CONS shall be provided by the X.25 Packet Level Protocol (PLP) [ISO 2]. The mapping of the elements of the CONS to the elements of the X.25 PLP is according to ISO 8878 [ISO 8]. This service shall be provided as specified in section 3.6.1 of the Workshop Agreements with the following modifications:

- o Section 3.6.1.3 does not apply.

When providing CONS in an ISDN, the considerations for control of B and D channels shall be provided by DIS 9574 [ISO 45] and implemented according to section 3.6.1.4 of the Workshop Agreements.

(Note that use of X.25 in GOSIP is consistent with FIPS 100-1 which requires CCITT X.25-1984, ISO 7776, and ISO 8202 until January 1, 1993. After that time, additional items covered in CCITT X.25-1988 are mandated by FIPS 100-1.)

4.2.3.3 Network Layer Protocol Identification

OSI systems require the ability to identify which OSI protocols and services are used in a particular instance of communication. These rules for identification are specified in ISO DTR 9577 [ISO 43]. GOSIP systems shall implement the protocol identification rules as specified in section 3.9.2.2 of the Workshop Agreements.

4.2.3.4 Special Provisions For Integrated Services Digital Networks

Integrated services digital networks (ISDN) enables X.25 PLP data to be sent across the D channel, sharing the channel with signaling data, and across a B channel. The Acquisition Authority must specify whether one or both of these capabilities are required. When operation of X.25 over a B channel is selected, the B channel can be provided as a switched service or a permanent service. The Acquisition Authority must specify whether one or both of these capabilities are required.

(Note that at the present time switched access to the B channel is available from most ISDN vendors, but not in a standard fashion; thus, multi-vendor interoperability between terminal equipment and switching equipment is not widely available today. Work underway in the North American ISDN Implementors' Workshop (IIW) is expected to improve this situation in the future. As appropriate IIW Agreements are developed, and related ISDN FIPS are issued by NIST, GOSIP will be updated accordingly.)

ISDN provides the possibility of a BRI (16 Kbps D-channel + 2 64 Kbps B-channels) or a PRI (64 Kbps D-channel + 23 64 Kbps B-channels). The Acquisition Authority must specify whether BRI or PRI is required for each system. The BRI service interface might be available at the S, T, or U reference point. The Acquisition Authority must specify the physical interface required for each BRI system.

ISDN B-channel services can be used by a GOSIP end system in any of six ways:

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.

The Acquisition Authority must specify the B-channel access capabilities required for any GOSIP end system intended for use with ISDN B-channel services.

For ISDN physical layer access at the S, T, and U reference points, sections 2.7.2.1 and 2.7.2.2 of the Workshop Agreements apply. For data link layer access on the D channel, section 2.7.2.4 of the Workshop

Agreements applies. For signaling on an ISDN interface, section 2.7.2.5 of the Workshop Agreements applies. For data link layer access on a B channel, section 2.7.2.6 of the Workshop Agreements applies. The PLP for use on ISDN B and D channels shall be implemented as specified in section 2.7.2.7 of the Workshop Agreements.

4.2.4 Transport Layer

For GOSIP end systems, the connection-oriented transport service (COTS), as provided by Transport class 4, is mandated for Government-wide interoperability and is the required means of providing a reliable end-to-end data communications path between end systems. The connectionless transport service (CLTS) is an option available for GOSIP end systems.

4.2.4.1 Connection-Oriented Transport Service

The vendor shall provide Transport class 4 [NIST 1; ISO 12,13] according to section 4.5.1 of the Workshop Agreements, with the modifications and additions stated below. Transport class 0 [NIST 1; CCITT 10,11] is to be used as appropriate in accordance with the CCITT X.400 recommendations (see section 4.2.7.3 of this profile).

Replace the sixth bullet of the Workshop Agreements section 4.5.1.2.1 with the following:

- o It is recommended that implementations not send user data in the CR or CC TPDU. Any user data received in a CR or CC TPDU will be made available to the Transport Service user.

Replace the seventh bullet of the Workshop Agreements section 4.5.1.2.1 with the following:

- o It is recommended that implementations not send user data in the DR TPDU. Any user data received in a DR TPDU will be made available to the Transport Service user.

Add, as the thirteenth bullet of the Workshop Agreements section 4.5.1.2.1, the following:

- o Transport expedited shall be provided as an optional service for the Transport Service user.

In specifying operator and higher layer protocol access controls in transport, the Acquisition Authority should be guided by the implementation guide and military supplement [NIST 5,6].

4.2.4.2 Connectionless Mode Transport Service

The Acquisition Authority may specifiy the optional connectionless mode transport service (CLTS) for GOSIP end systems [ISO 46]. This option may be specified only as an addition to the connection-oriented transport service. Although no GOSIP mandated protocols require the CLTS, a number of non-GOSIP protocols widely available in industry can use CLTS as an efficient means of communicating across local area networks. The Acquisition Authority must determine the need for CLTS to support non-GOSIP protocols.

The CLTS option shall be implemented using IS 8602 [ISO 47] according to section 4.6 of the Workshop Agreements [NIST 1].

4.2.5 Session Layer

The vendor shall provide the Session protocol as specified in section 5.9 and section 5.12 of the Workshop Agreements. Application layer protocols determine the session layer functional units needed for their support. Current and future needs should be considered when selecting Session layer functional units. [NIST 1; ISO 14,15; CCITT 12,13].

4.2.6 Presentation Layer

The vendor shall provide the Presentation protocol as specified in section 5.8 and section 5.12 of the Workshop Agreements. See References [NIST 1; ISO 20, 21, 24, 25].

4.2.7 Application Layer

4.2.7.1 Association Control Service Elements (ACSE)

The ACSE, as specified in section 5.5 and section 5.12 of the Workshop Agreements, is required to support all applications except Message Handling Systems. See section 4.2.7.3 of this profile. See References [NIST 1; ISO 22-25]. Section 5.12.1.1 of the Workshop Agreements defines a fixed value for the Application Entity (AE) Title in order to satisfy the FTAM requirement for exchanging fields of this type; however, for compatibility with non-GOSIP systems, and to ease compatibility with future versions of GOSIP, GOSIP systems must allow locally configurable AE Titles to be generated and received.

4.2.7.2 File Transfer, Access, and Management Protocol (FTAM)

The following categories of FTAM systems are defined for procurement purposes: (1) limited-purpose systems, and (2) full-purpose systems. These categories are defined by their support requirements given below. All FTAM systems in these categories are bound by the language and conditions for Phase 2 FTAM implementations contained in section 9 of the Workshop Agreements. [NIST 1] (Hereafter section 9.)

A limited-purpose FTAM system provides the functions of simple file transfer and management. Such a system must support at least Implementation Profiles T1 (Simple File Transfer) and M1 (Management) as defined in section 9. Support requirements for Implementation Profiles are given in Table 9.7 of section 9. A full-purpose FTAM system provides the functions of positional file transfer (including simple file transfer), simple file access, and management. Such a system must support at least Implementation Profiles T2 (Positional File Transfer), A1 (Simple File Access), and M1 (Management), as these are defined in section 9. A limited-purpose FTAM system is able to interoperate with a full-purpose FTAM system at the intersection of their capabilities.

FTAM implementations (whether full-purpose or limited-purpose) can operate as an initiator of remote file activity, as a responder to requests for remote file activity, or as both initiator and responder. Further, FTAM implementations can operate as senders (of data to receivers), receivers (of data from senders), or as both. Thus, any of four possible roles may be assumed as follows: initiator-sendor, initiator-receiver, responder-sender, and responder-receiver. The Acquisition Authority must determine the requirements for each FTAM device and must specify such requirements in terms of initiator, responder, sender, and receiver, as well as in terms of limited-purpose or full-purpose.

4.2.7.3 Message Handling Systems

The vendor shall provide all Message Transfer Services and Interpersonal Messaging Services specified in section 7 of the Workshop Agreements. [NIST 1] Communication between two Message Transfer Agents, one or both of which reside entirely and exclusively within a public message domain administered by a public data network, takes place as specified by CCITT Recommendation X.410 (1984). CCITT mandates that transport class 0 and the Connection Oriented Network Service (CONS) [ISO 2, 3] be used by end systems when messaging over public messaging domains on public data networks. All end systems on private management domains must use transport class 4. Private management domain end systems that are also connected to public messaging domains conforming to CCITT Recommendation X.410 must also implement and use transport class 0 when acting as a messaging relay between the two domains. Specifically, the Message Transfer Agent in the system connected to both the private and public messaging domain performs the relay; there is no transport relay involved.

4.2.7.4 Virtual Terminal (VT) Basic Class

The following categories of VT systems are defined for procurement purposes: 1) simple systems, and 2) forms capable systems. All VT systems in these categories are bound by the language and conditions contained in section 14 of the Workshop Agreements.

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

A forms-capable system is intended to support forms-based applications with local entry and validation of data by the terminal system. A forms-capable system supports functions such as "cursor movement," "erase screen," and "field protection." A forms-capable system supports the forms profile specified in section 14.8.3 of the Workshop Agreements. The forms profile requires the Synchronous mode (S-mode) of operation and specifies simple delivery control.

The Basic Class VT International Standard [ISO 32] specifies three negotiation options which are independent of the VT profiles. These are No Negotiation, Switch Profile, and Multiple Interaction Negotiation. Multiple Interaction Negotiation is not addressed by the Workshop Agreements, but any system claiming support of this negotiation option must also support the Switch Profile and No Negotiation options. Any system supporting Switch Profile Negotiation must also support the No Negotiation option. Seven bit USASCII, as well as the International Reference Version (IRV) of ISO-646 graphic repertoires, must be supported by both simple and forms capable systems.

4.2.8 Exchange Formats

Exchange formats are not OSI standards. They are included in GOSIP because the information that they describe can be transported by the OSI FTAM and MHS protocols either as the content of a file or as the body part of a message. The GOSIP contains only that information about exchange formats that are required to provide this capability. For detailed specifications on the exchange formats, consult the appropriate standards documents or the Workshop Agreements.

Version 2 of GOSIP includes information on how to identify and transport the ODA exchange format. Future versions of GOSIP will include information on how to identify and transport additional formats such as Computer Graphics Metafile (CGM) and the Standard General Markup Language (SGML). For further details, see Appendix 4.

ODA information can also be transported by other mechanisms which are outside the scope of the GOSIP.

4.2.8.1 Office Document Architecture (ODA)

The ODA Standard [ISO 36-42, CCITT 17-24] specifies rules for describing the logical and layout structures of documents as well as rules for specifying character, raster, and geometric content of documents, thus, providing for the interchange of complex documents. The interchanged documents may be in formatted form (i.e., for presentation such as printing, displaying), in processable form (i.e., for further processing such as editing) or in formatted processable form (i.e., for both presentation and further processing).

To transfer an ODA file, the services provided by either the MHS or FTAM application can be used.
If the MHS application is used, OdaBodyParts are encoded for transmission over a CCITT X.400-1984 service as a single body part with tag 12 in the P2 protocol.

```
Oda [12] IMPLICIT OCTETSTRING
```

The content of the OCTETSTRING is a SEQUENCE of OdaBodyPart Parameters and OdaData components with a value of type OdaBodyPart.

```
OdaBodyPart :: = SEQUENCE {
   OdaBodyPart Parameters,
   OdaData              }
```

The OdaBodyPart Parameters component is a SET containing the document-application-profile and the document-architecture-class identifiers

```
OdaBodyPart Parameters :: = SET {
   document-application profile [0] IMPLICIT OBJECT IDENTIFIER
   document-architecture-class [1] IMPLICIT INTEGER {
                 formatted (0),
```

processable (1),
formatted-processable (2) }}

The OdaData component is a SEQUENCE of Intercharge-Data Element as defined by IS 8613-5 [ISO 39]

OdaData :: = SEQUENCE of Interchange-Data-Element

In the P1 protocol, both the undefined bit (bit 0) and the ODA bit (bit 10) of the Encoded Information Type must be set when an ODA document is present in P2.

When using FTAM to transfer an ODA file, the FTAM-3 (ISO FTAM unstructured binary) document type should be specified; however, since files that are not ODA files can have the same document type, it is left up to the user of application programs that remotely access files using FTAM to know that a given file contains ODA information.

4.3 INTERMEDIATE SYSTEM SPECIFICATION

Intermediate systems shall operate in connectionless mode. That is, the connectionless network protocol is used regardless of whether the underlying technology operates in connectionless (e.g., CSMA/CD, token ring) or connection-oriented (e.g., X.25, LAP B) mode; however, the connectionless mode need not be used to interconnect X.25 subnetworks to form a single logical subnetwork. Also note that local area network bridges may be employed to form a single logical subnetwork.

Intermediate systems may use any combination of the lower layer technologies as specified in the above sections of this profile: 4.2.1 Physical Layer, 4.2.2 Data Link Layer, and 4.2.3 Network Layer. That is, agencies may interconnect local and wide area networks. Implementation profiles for these protocols are contained in the Workshop Agreements and are referenced in the above sections of this profile. Implementation specifications for connectionless-mode intermediate systems are given in section 3.5 of the Workshop Agreements.

Addressing structure and Address Registration Authorities are specified in section 5 of this profile.

A system that serves as both end system and intermediate system must satisfy the mandatory requirements of sections 4.2 and 4.3 of this profile.

5. ADDRESSING REQUIREMENTS

5.1 NETWORK LAYER ADDRESSING AND ROUTING

This section specifies the Network Layer addressing scheme and its administrative and routing implications. It also identifies authorities responsible for the administration of the scheme and how subauthorities will be assigned and which responsibilities shall be delegated to them.

5.1.1 NSAP Address Administration, Routing Structures and NSAP Address Structure

Network Service Access Point (NSAP) addresses specify the points where the communication capability of the Network Layer (i.e., the Network Service) is made available to its users. In effect they address the direct users of the Network Service, normally transport entities. The semantics of NSAP addresses are encoded into Network Protocol Address Information (NPAI) and conveyed in the appropriate protocol data units (PDUs) between protocol entities providing the Network Service.

The basic principles of Network Layer addressing, as defined in Addendum 2 to the Network service definition [ISO 5], include:

- o NSAP address administration is based on the concept of hierarchical Addressing Domains. An Addressing Domain is a set of addresses interrelated by virtue of being administered by a common authority. The term authority refers to the entity that specifies the structure and ensures the uniqueness of identifiers in the associated domain. In practice the structure of NSAP addresses reflects this administrative hierarchy in that, at any level of the hierarchy, an initial part of the address unambiguously identifies the Addressing (sub) Domain.

  - o The first three levels of the NSAP addressing domain are standardized and result in the NSAP address structure in Figure 5.1.1. The Initial Domain Part (IDP) of the address consists of two parts, the Authority and Format Identifier (AFI) and the Initial Domain Identifier (IDI). The AFI specifies the format of the IDI, the authority that is responsible for allocating IDI values, and the syntax used to represent the Domain Specific Part (DSP). The IDI is interpreted according to the value of the AFI and its value identifies the authority responsible for the structure and assignment of DSP values. The DSP is allocated and assigned by the authority specified by the IDP part.

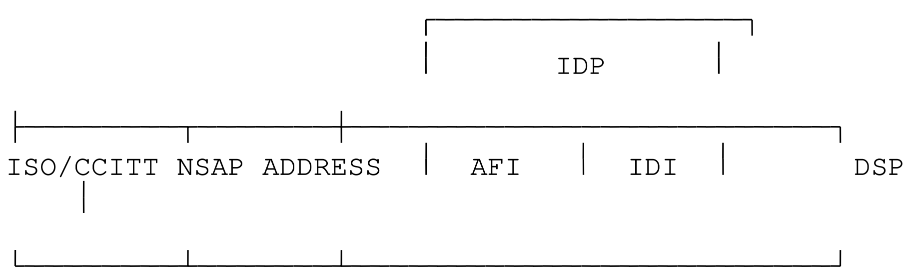

Figure 5.1.1 NSAP Address Structure

The National Institute of Standards and Technology (NIST) has been designated as the authority to administer the addressing domain identified by IDI value 0005 under AFI 47. The AFI value of decimal 47 specifies that the IDI part is interpreted as a four decimal digit International Code Designator (ICD) and that the DSP has a binary abstract syntax. ICDs are allocated and assigned by ISO [ISO 27] and identify international organizations that are the authorities for address administration for an addressing subdomain.

The addressing domain identified by ICD 0005 shall be available for use by all of the Federal Government. The NIST shall specify the structure and semantics of the DSP associated with ICD 0005 and delegate the task of administering the assignment of DSP values to the General Services Administration (GSA). This is summarized in Figure 5.1.2.

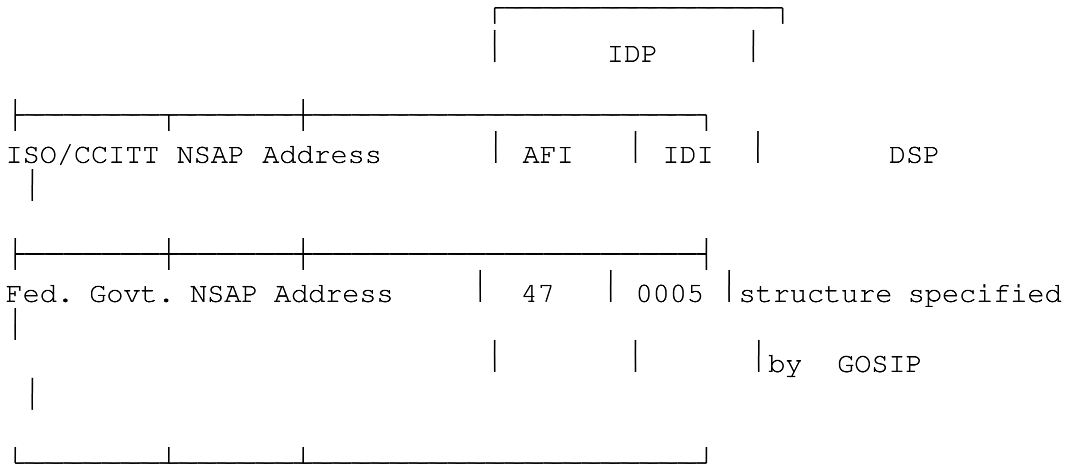

Figure 5.1.2 The NIST ICD Addressing Domain

NSAP addresses, encoded as NPAI in appropriate NPDUs, serve as the primary input to the routing and relaying functions of protocol entities providing the Network Service. As such, the semantics of NSAP addresses must convey information required for routing as well as address administration.

The basic principles of Network Layer routing, as defined in the OSI Routing Framework [ISO 48], include:

- o The global OSI environment will consist of a number of Administrative Domains. An Administrative Domain consists of a collection of End Systems (ESs) and Intermediate Systems (ISs), and subnetworks operated by a single entity or Administrative Authority. The Administrative Authority is responsible for the organization of ESs and ISs into Routing Domains; the further structuring and assignment of NSAP addresses; the policies that govern the information that is collected and disseminated both internally and externally to the Administrative Domain; and, the establishment of subdomains and the corresponding delegation of responsiblities.

- o A Routing Domain is a set of ESs and ISs which operate according to the same routing procedures and which is wholly contained within a single Administrative Domain. An Administrative Authority may delegate to the entity responsible for a Routing Domain the responsibilities to further structure and assign NSAP addresses. The hierarchical decomposition of Routing Domains into subdomains may greatly reduce the resources required in the maintenance, computation and storage of routing information.

This GOSIP makes provisions for the establishment of Administrative Domains, Routing Domains and one level of routing subdomains (called Areas). This decomposition of the routing environment allows, where appropriate, administrative entities to request the delegation of responsibility for the organization and administration of their systems and subnetworks. The provision of two levels of routing structures within an Administrative Domain will allow Administrative Authorities to engineer routing configurations that best serve their individual needs.

Figure 5.1.3 depicts the GOSIP NSAP address structure. This structure is mandatory for addresses allocated from the ICD 0005 addressing domain.

```
        IDP

 AFI    IDI                                      DSP

 47     0005       DFI      Admin Author.     Reserved     Routing Domain
 Area       System        NSel

Octets    1      2          1             3            2               2
   2          6          1
```

Figure 5.1.3 GOSIP NSAP Address Structure

The DSP Format Identifier (DFI) specifies the structure, semantics and administration requirements associated with the remainder of the DSP. This field provides for graceful support of future DSP structures should the need arise. Currently, only one DSP format (DFI=10000000) is defined under ICD 0005. The remainder of this section describes this DSP format.

The Administrative Authority field identifies the entity that is responsible for the organization of ISs and ESs into Routing Domains and Areas; the allocation and assignment of the remaining portion of the DSP; and the policies that govern the dissemination of information within and external to the Administrative Domain. Note that it is unlikely that a large number of Federal Government organizations will establish their own Administrative Domains. Instead, it is more likely that Administrative Domains will be established for collective organizations that autonomously operate large inter-networks and that individual organizations would correspondingly be delegated authority for Routing Domains or Areas.

The Reserved field is positioned to be available for encoding higher level routing structures above those of the routing domain or to be used to expand either the Administrative Authority or the Routing Domain fields in future DSP formats should the need arise.

The Routing Domain field identifies a unique Routing Domain within an Administrative Domain.

The Area field identifies a unique subdomain of the Routing Domain.

The System field identifies a unique system (ES or IS) within an Area. The format, value, structure and meaning of this field is left to the discretion of its administrator.

The NSAP Selector field identifies a direct user of the Network Layer service, usually a Transport entity. (The NSAP Selector may also identify other direct users of the Network Service if required by the Acquisition Authority.) GOSIP allows a system administrator to configure NSAP Selector-to-Transport entity mappings because, for example, several transport entities may co-exist in some systems.

5.1.2 NSAP Address Registration Authorities

This section names the GSA as the GOSIP Address Registration Authority, and specifies how subauthorities shall be assigned, and which responsibilities transfer to them.

Under its delegated authority as Address Registration Authority for ICD 0005, GSA shall, upon request, assign, maintain, and publicize unique Administrative Authority identifiers for Federal Government entities that require distinct Administrative Domains. Contact GSA at:

Telecommunications Customer Requirements Office
U. S. General Services Administration
IRMS
Office of Telecommunications Services
18th & F Sts. N.W.
Washington, D. C. 20405

for the procedures for requesting the assignment of an Administrative Authority identifier. They are also included in Version 2 of the GOSIP User's Guide.

5.1.2.1 Responsibilities Delegated by NIST

The management responsibilities delegated by the NIST, via the GSA, to Federal Government entities issued an Administrative Authority identifier under ICD 0005 are given below.

- o The entity must designate and register with the GSA a specific point of contact for its Administrative Authority.
- o The entity must ensure that procedures exist to establish appropriate routing structures and to delegate, if required, responsibliities to the administrators of individual Routing Domains or Areas.
- o The entity must ensure that addresses are assigned uniquely and are kept current and accurate.
- o The entity must ensure that policies are defined and procedures exist for making addresses and routing information known to other administrative domains.
- o The entity may, on a voluntary basis, supply such information to the GSA for government-wide compilation and dissemination. The GOSIP Users' Guide [NIST 7] lists the factors that Administrative Authorities should consider before requesting this service and the procedures to be followed if the service is required.

5.1.3 GOSIP Routing Procedures

This GOSIP specifies dynamic routing procedures for the exchange of configuration information between ESs and ISs connected via local area and point to point (pt-pt) subnetworks and hierarchical, static routing procedures for the establishment of routing information among ISs. These routing procedures shall be provided according to section 3.8 of the Workshop Agreements, with the following additions after the paragraph of section 3.8.2:

- o The Routing Information Base (RIB) shall be capable of associating arbitrary sets of NSAPs, described as NSAP address prefixes, with next hop forwarding information for use by the ISO 8473 Route PDU Function. In addition, the RIB must be capable of supporting a default entry that is used in forwarding PDUs containing destination NSAP addresses that do not match any other RIB entries.

Nonstandard dynamic routing procedures, in addition to the static capabilities specified above, may be used to establish RIBs within ISs in the interim period while OSI IS-IS dynamic routing protocols are still under development. It should be noted that the GOSIP supported routing structures and DSP addressing structure are in alignment with the OSI IS-IS intra-domain routing protocol [ISO 49] currently under development and that later versions of this profile will mandate the use of standardized OSI IS-IS routing protocols.

The routing procedures required for GOSIP systems to communicate with non-GOSIP OSI-compliant systems are discussed in Version 2 of the GOSIP User's Guide.

5.2 UPPER LAYERS ADDRESSING

The following sections provide guidance on certain upper layer addressing issues.

5.2.1 Address Structure

The address structure for the Session Service Access Point (SSAP) and Transport Service Access Point (TSAP) Selector is two octets for each field, encoded in binary as shown on Fig. 5.2.1. Other lengths conforming to the limits specified in the Workshop Agreements, may be assigned by an end system administrator.

PSAP	SSAP	TSAP
binary	binary	binary
2 octets	2 octets	2 octets

Figure 5.2.1 Upper Layers Address Structure

5.2.2 Address Assignments

Service access point (SAP) selectors specify the addresses of standard service interfaces. Values are assigned by an end system administrator and must be configurable in GOSIP end systems. T-selectors and S-selectors are each encoded as a string of octets. The octet string may be specified as an unsigned integer; if so, the high order octet precedes low order octets. P-selectors are encoded in Abstract Syntax Notation (ASN).1 type OCTETSTRING as per the Presentation protocol specification [ISO 21].

The Application Context Name can be used to distinguish the Application entities that use the common application services of ACSE. The Application Context Names for FTAM and VT, as specified in sections 5.12.1.1 and section 5.12.1.4 of the Workshop Agreements, are "ISO FTAM" and "ISO VT." Note that applications which require additional Application Context information may define them, even if they make use of FTAM and/or VT.

5.2.3 Address Registration

As an interim measure, until Directory Service implementations are available, federal agencies that wish to have their PSAP address (upper layer SAP selector values plus full NSAP address) accessible to other agencies may register these addresses with GSA. GSA shall catalog, maintain, and disseminate these addresses.

5.3 IDENTIFYING APPLICATIONS

5.3.1 FTAM and File Transfer User Interface Identification

The FTAM service definition [ISO 18] includes an optional parameter called the initiator identity. GOSIP recommends the use of this parameter in FTAM implementations to identify users of the service. Generally, an identifying name or group of names is provided in this field. The name identifies the particular user in such a way that two different users may readily be distinguished. In the standard there are no restrictions on what may be included. The initiator identity is encoded as an ASN.1 [ISO 25] variable length graphic string with characters from the ISO646 set [ISO 9]. These names are normally inserted as needed by end systems, and this profile makes no provision for registration. The content is system-dependent.

5.3.2 MHS and Message User Interface Identification

The MHS Recommendations [CCITT 2-9] identify a user to a Message Transfer Agent by means of a parameter called the Originator/Recipient Name (O/R Name). The O/R Name is encoded as a set of attributes describing the originator and receiver of the message. The attributes which must be supported by all implementations are the country name, the administration name, private domain name, organization name, organizational units, and personal name. The administration name attribute shall contain one blank when the originator and/or recipient are attached only to a private domain. The private domain name attribute must also be supported by all implementations, and be included when the originator and/or the recipients are located within different private domains. This information is summarized in Table 5.3.

Attribute	Maximum ASCII Character Length
country name	3
administration name	16
private domain name	16
organization name	64
sequence of org. units	32 each
personal name	64

Table 5.3 Required O/R Name Attributes

Private messaging systems within the government shall be capable of routing on the administration name, private domain name, organization name and organizational unit attributes taken in their hierarchical order. They shall also be capable of routing on or delivering based on the personal name attribute; that is, they shall act as Class 2 or Class 3 MTAs as defined in section 7.7.3.3 of the Workshop Agreements. The General Services Administration (GSA) shall be the Address Registration Authority for organization names. GSA shall delegate Address Registration Authority to the organization indicated by the organization name to assign organization unit and personal names. In assigning the organizational unit personal name space, the Address Registration Authorities shall follow the same rules stated earlier for NSAP addresses, except that organizational unit and personal names are not registered with GSA. Typically, a unique personal name is a surname or surname followed by given name, but it could also be an identifier of a particular office within the organization unit.

CCITT assigns country name and administration name to public message service providers. Administrations assign private domain names to private messaging systems that wish to interoperate across the administration. The administration may also provide a registration service for government assigned organization names that wish to interoperate across or between administrative domains. A method for assigning private domain names in the absence of an administrative name is given in section 8.4.2 of Version 2.0 of the GOSIP User's Guide.

6. SECURITY OPTIONS

Security is of fundamental importance to the acceptance and use of open systems in the U.S. Government. Part 2 of the Open Systems Interconnection reference model (Security Architecture) is now an International Standard (IS 7498/2). The standard describes a general architecture for security in OSI, defines a set of security services that may be supported within the OSI model, and outlines a number of mechanisms than can be used in providing the services. However, no protocols, formats or minimum requirements are contained in the standard.

The text below describes one security option that may be optionally specified when security services are incorporated in the OSI network layer. This chapter does not describe at this time a complete set of security options that a user might desire nor a description of the security services and protocols that are associated with the specified parameter. It is a parameter that has been identified as being needed if certain security services (e.g., confidentiality, access control) are incorporated in the network layer. The parameter should be used where required, but this chapter should be considered as a placeholder for future security specifications. Appendix 1 provides further information on what specifications are considered needed for OSI security.

As defined by ISO, security features are considered both implementation and usage options. An organization desiring security in a product that is being purchased in accordance with this profile must specify the security services required, the placement of the services within the OSI architecture, the mechanisms to provide the services and the management features required. An acquisition authority desiring Connectionless Network Protocol (CLNP) security should specify the following described security option(s). When specifying the CLNP security option, the acquisition authority must ensure that all necessary Security Format Codes are provided.

6.1 REASON FOR DISCARD PARAMETERS

The implementation of the security option requires assigning new parameter values to the Reason for Discard parameter in the CLNP Error Report PDU. The first octet of the parameter value contains an error type code as described in IS 8473. Values beyond those assigned in the standard are shown in Table 6.1. The second octet of the Reason for Discard parameter value either locates the error in the discarded PDU or contains the value zero as described in the standard.

Parameter Values			
Octet 1 Bits 8765 4321	Octet 2 Bits 8765 4321	Class of Error	Meaning
1101 0000	Discarded PDU	Security	Security Option

	Offset or Zero		Out-of-Range
1101 1010	0000 0000	Security	Basic Portion Missing
1101 1101	0000 0000	Security	Extended Portion Missing
1101 0010	0000 0000	Security	Communication Administratively Prohibited

Table 6.1 Extended Values in the Reason For Discard Parameter

6.2 SECURITY PARAMETER FORMAT

IS 8473 defines the format of the CLNP security parameter. This parameter consists of the three fields shown in Table 6.2.

Octets	Bits 8765 4321	
N	1100 0101	Parameter Code
N + 1	Len = M	Parameter Length
N + 2 N + M + 1		Parameter Value

Table 6.2 Security Parameter Format

6.2.1 Parameter Code

IS 8473 assigns the value "1100 0101" to the Parameter Code field to identify the parameter as the Security Option.

6.2.2 Parameter Length

This octet indicates the length, in octets, of the Parameter Value field.

6.2.3 Parameter Value

The Parameter Value field contains the security information. IS 8473 defines only the first octet of the Parameter Value field. This section completes the definition of this field. Table 6.3 illustrates the format of the Parameter Value field within the Security Parameter.

Octets	Bits 8765 4321	
N	1100 0101	Parameter Code
N+1	Len = B + E + 1	Parameter Length
N+2	XX00 0000	Security Format Code
N+3 Parameter Value N+B+2		Basic Portion (Optional)
N+B+3		Extended Portion (Optional)

N+B+E+2		

Table 6.3 Format - Parameter Value Field

6.2.3.1 Security Format Code

As described in IS 8473, the high order two bits of the first octet of the Parameter Value field specify the Security Format Code. The standard reserves the remaining six bits and specifies that they must be zero.

6.2.3.2 Basic Portion

The Basic Portion of the Security Option identifies the U.S. classification level to which a PDU is to be protected and the authorities whose protection rules apply to that PDU. This portion is optional and appears at most once in a PDU. When the Basic Portion appears in the Security Option of a PDU, it must be the first portion in the Parameter Value field of the Security Parameter. Paragraph 6.3 defines the format of the Basic Portion.

6.2.3.3 Extended Portion

The Extended Portion permits additional security labelling information, beyond that present in the Basic Portion, to be supplied in a CLNP PDU to meet the needs of registered authorities. This portion is optional and appears at most once in a PDU. The Extended Portion must follow the Basic Portion, if present, in the Parameter Value field of the CLNP Security Parameter. In addition, if this portion is required by an authority for a specific system, it must be specified explicitly in any Request for Proposal for that system. Paragraph 6.4 defines the format of the Extended Portion.

6.3 BASIC PORTION OF THE SECURITY OPTION

The Basic Portion is used by the components of an internetwork to:

A. Transmit from source to destination, in a network standard representation, the common security labels required by computer security models.

B. Validate the PDU as appropriate for transmission from the source and delivery to the destination.

C. Ensure that the route taken by the PDU is protected to the level required by all protection authorities indicated on the PDU.

Table 6.4 shows the format of the Basic Portion of the Security Option.

Octets	Bits 8765 4321	
N	1000 0010	Basic Type Indicator
N+1	Len = I	Length of Basic Information
N+2 N+I+1		Basic Information

Table 6.4 Format - Basic Portion

6.3.1 Basic Type Indicator

The value of this field identifies this as the Basic Portion of the Security Option.

6.3.2 Length of Basic Information

This length field, when present, indicates the length, in octets, of the Basic Information field. The Basic Information field is variable in length and has a minimum length of two octets.

6.3.3 Basic Information

The Basic Information field consists of two subfields as Table 6.5 illustrates.

Octets	Bits 8765 4321		
B	1000 0010		Basic Type Indicator
B + 1	Len = F + 1		Length of Basic Information (Minimum = 2 Octets)
B + 2		Basic Information	Classification Level
B + 3 ... B + F + 2		Basic Information	Protection Authority Flags

Table 6.5 Format - Basic Information Field

6.3.3.1 Classification Level

The Classification Level field specifies the U.S. classification level to which the PDU must be protected. The information in the PDU must be treated at this level unless it is regraded in accordance under the procedures of all the authorities identified by the Protection Authority Flags. The field is one octet in length. Table 6.6 provides the encodings for this field.

VALUE Bits 8765 4321	LEVEL
0000 0001	RESERVED 4
0011 1101	TOP SECRET
0101 1010	SECRET
1001 0110	CONFIDENTIAL
0110 0110	RESERVED 3
1100 1100	RESERVED 2
1010 1011	UNCLASSIFIED
1111 0001	RESERVED 1

Table 6.6 Classification Levels

6.3.3.2 Protection Authority Flags

The Protection Authority Flags field indicates the National Access Program(s) or Special Access Program(s) whose rules apply to the protection of the PDU. Its field length and source flags are described below. To maintain the architectural consistency and interoperability of DoD common user data networks, users of these networks should submit requirements for additional Protection Authority Flags to DCA DISDB, Washington, D. C. 20305-2000 for review and approval.

A. Field Length: The Protection Authority Flags field is variable in length. The low order bit (Bit 1) of an octet is encoded as "0" if the octet is the final octet in the field. If there are additional octets, then the low order bit is encoded as "1". Currently, there are less than eight authorities. Therefore, only one octet is required and the low order bit of this octet is encoded as "0".

B. Source Flags: Bits 2 through 8 in each octet are flags. Each flag is associated with an authority as indicated in Table 6.7. The bit corresponding to an authority is "1" if the PDU is to be protected in accordance with the rules of that authority.

Bit Number	Authority	Point of Contact
8	GENSER	Designated Approving Authority per DoD 5200.28
7	SIOP-ESI	Department of Defense

		Organization of the Joint Chiefs of Staff Attn: J6T Washington, D.C.
6	SCI	Director of Central Intelligence Attn: Chairman, Information Handling Committee Intelligence Community Staff Washington, D. C. 20505
5	NSA	National Security Agency 9800 Savage Road Attn: TO3 Ft. Meade, MD 20755-6000
4	DOE	Department of Energy Attn: DP343.2 Washington, D.C. 20545
3 , 2	Unassigned	
1	Extension Bit	Presently always "O"

Table 6.7 Protection Authority Bit Assignments

6.4 EXTENDED PORTION OF THE SECURITY OPTION

Table 6.8 illustrates the format for the Extended Portion. To maintain the architectural consistency of DoD common user data networks, and to maximize interoperability, users of these networks should submit their plans for the use of the Extended Portion of the Security Option to DCA DISDB, Washington, D.C. 20305-2000 for review and approval. Once approved, DCA DISDB will assign Additional Security Information Format Codes to the requesting activities.

Octets	Bits 8765 4321	
N	1000 0101	Extended Type Indicator
N+1	Len = I	Length of Extended Information
N+2 … N+I+1		Extended Information

Table 6.8 Format - Extended Portion

6.4.1 Extended Type Indicator

The value of this field identifies this as the Extended Portion of the Security Option.

6.4.2 Length of Extended Information

This length field indicates the length, in octets, of the Extended Information field. The Extended Information field is variable in length with a minimum length of two octets.

6.4.3 Extended Information

The Extended Information field consists of three subfields as Table 6.9 illustrates. These three fields form a sequence. This sequence may appear multiple times, forming a set, within the Extended Information field.

```
                         Bits 8765  4321
           Octets
           E                1000  0101     Extended Type Indicator

           E+1      Len = (B - A) + 1      Length of Extended Information
                                             (Minimum = 2 Octets)

     A     E+2                             Additional Security Information Format Code

           E+3      Len = I                Length of Additional Security Information

           E+4
                                           Additional Security Information
           E+I+3                           (Zero or more octets)

              (Additional Sequences
 Extended     of the above three fields)
 Information

           E+N                             Additional Security Information Format Code

           E+N+1    Len = J                Length of Additional Security Information

           E+N+2
                                           Additional Security Information
     B     E+N+J+1                           (Zero or more octets)
```

Table 6.9 Format - Extended Information Field

6.4.3.1 Additional Security Information Format Code

The value of the Additional Security Information Format Code corresponds to a particular format and meaning for a specific Additional Security Information field. Each format code is assigned to a specific controlling activity. Once assigned, this activity becomes the authority for the definition of the remainder of the Additional Security Information identified by that format code. A single controlling activity may be responsible for multiple format codes. However, a particular format code may appear at most once in a PDU. For each Additional Security Information Format Code an authority is responsible for, that authority will provide sufficient criteria for determining whether a CLNP PDU marked with its Format Code should be accepted or rejected. Whenever possible, this criteria will be Unclassified.

Note: The bit assignments for the Protection Authority flags of the Basic Portion of the Security Option have no relationship to the "Additional Security Information Format Code" of this portion.

6.4.3.2 Length of Additional Security Information

This field provides the length, in octets, of the "Additional Security Information" field immediately following.

6.4.3.3 Additional Security Information

The Additional Security Information field contains the additional security relevant information specified by the authority identified by the "Additional Security Information Format Code." The format, length, content, and semantics of this field are determined by that authority. The minimum length of this field
is zero.

6.5 USAGE GUIDELINES

A PDU is "within the range" if

MIN-LEVEL <= PDU-LEVEL <= MAX-LEVEL

where MIN-LEVEL and MAX-LEVEL are the minimum and maximum security levels, respectively, that the system is accredited for. The term PDU-LEVEL refers to the security level of the PDU. In this context, the "security level" may involve the combination of three factors:

1) classification level
2) protection authorities
3) additional security labelling information as required and defined by the responsible activity.

The authorities responsible for accrediting a system or collection of systems are also responsible for determining whether and how these factors interact to form a security level or security range. A PDU should be accepted for further processing only if it is within range. Otherwise, the Out-of-Range procedure described in Paragraph 6.6 should be followed.

6.5.1 Basic Portion of the Security Option

Use of the information contained in the Basic Portion of the Security Option requires that an end system be aware of:

A. the classification level, or levels, at which it is permitted to operate, and

B. the protection authorities responsible for its accreditation.

Representation of this configuration information is implementation dependent.

6.5.2 Extended Portion of the Security Option

Use of the Extended Portion of the Security Option requires that the end system configuration accurately reflects the accredited security parameters associated with communication via each network interface. Representation of the security parameters and their binding to specific network interfaces is implementation dependent.

6.6 OUT-OF-RANGE PROCEDURE

If the Out-Of-Range condition was triggered by:

A. A required, but missing, Security Option or Basic or Extended Portion of a Security Option, then the PDU should be discarded. In addition, a CLNP Error Report or other form of reply is not permitted in this case. However, a local security policy may permit data to be delivered or a CLNP Error Report PDU to be processed provided a reply is not sent.

B. A PDU whose security level is less than the end system's minimum security level, then the PDU should be discarded. In addition, a CLNP Error Report or other form of reply is not permitted in this case. However, local security policy may permit data to be delivered or a CLNP Error Report PDU to be processed provided a reply is not sent.

C. A PDU whose security level is greater than the end system's maximum security level, then:

1. If a CLNP Error Report PDU triggered the Out-of-Range condition, then no reply is permitted and the PDU should be discarded. A CLNP Error Report PDU must not be sent in this case.

2. Otherwise, discard the PDU and send a CLNP Error Report PDU to the originating CLNP entity. The first octet of the Reason for Discard parameter is set as specified in Table 6.1. The second octet of the Reason for Discard parameter identifies the Out-of-Range portion of the Security Option. It should point to the first octet (i.e., the type indicator) of the Out-of-Range portion. Alternatively, the second octet can be set to zero. The response is sent at the maximum classification level of the end system which received the PDU. The protection authority flags are set to be the intersection of those for which the host is accredited and those present in the PDU which triggered this response.

Example: PDU = "Secret, GENSER"
End System Level = "Unclassified, GENSER".
Reply = "Unclassified, GENSER".

These are the least restrictive actions permitted by this protocol. Individual end systems, system administrators, or protection authorities may impose more stringent restrictions on responses and in some instances may not permit any response at all to a PDU which is outside the accredited security range of an end system.

6.7 TRUSTED INTERMEDIARY PROCEDURE

Certain devices in an internetwork may act as intermediaries to validate that communications between two end systems is authorized. This decision is based on a combination of knowledge of the end systems and the values in the CLNP Security Option. [The Blacker Front End (BFE) is one example of such a trusted device.] These devices may receive CLNP PDUs which are in range for the intermediate device, but are either not within the accredited range for the source or the destination. In the former case, the PDU should be treated as described in Paragraph 6.6. In the latter case, a CLNP Error Report PDU should be sent to the originating CLNP entity. The first octet of the Reason for Discard parameter should be set to 1101 0010. This code indicates to the originating CLNP entity that communication with the end system is administratively prohibited (refer to Table 6.1). The security range of the interface on which the reply will be sent determines whether a reply is allowed and at what security level it should be sent.

REFERENCES

National Institute of Standards and Technology

1. NIST Special Publication 500-177, Stable Implementation Agreements for Open Systems Interconnection Protocols, Version 3. This document can be purchased from National Technical Information Service (NTIS), U. S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161. For telephone orders call: (703) 487-4650. This document may also be purchased from the IEEE Computer Society, Order Department, phone: 1-800-272-6657.

2. FIPS l07, Local Area Networks: Baseband Carrier Sense Multiple Access with Collision Detection Access Method and Physical Layer Specifications and Link Layer Protocol, NTIS, U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22l6l.

3. FIPS l00, Interface Between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) For Operation With Packet-Switched Data Communications Networks, NTIS, U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22l6l.

4. Implementation Agreements Among Participants of OSINET, NBSIR 89-4158, National Institute of Standards and Technology.

5. Military Supplement to ISO Transport Protocol, National Institute of Standards and Technology, National Computer Systems Laboratory, ICST/SNA-85-17, 1985.

6. Implementation Guide for ISO Transport Protocol, National Institute of Standards and Technology, National Computer Systems Laboratory, ICST/SNA-85-18, 1985.

7. NIST Special Publication 500-163 Government Open Systems Interconnection User's Guide. This document can be purchased from the National Technical Information Service (NTIS), U. S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161. For telephone orders call (7023) 487-4650. The NTIS order number is PB90-111212.

8. GOSIP Conformance and Interoperation Testing and Registration, NCSL/SNA 90-2, 1990.

9. NIST Special Publication 500-182, Message Handling Systems Implementation Evaluation Guidelines. See [NIST 7] for NTIS ordering information.

National Communications System

Federal Standard FED-STD 1041, Interface Between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) For Operation With Packet-Switched Data Communications Networks, National Communications System.

Institute of Electrical and Electronic Engineers, Inc.

Binary Floating Point Arithmetic (ANS1 Approved), IEEE 754, March 21, 1985, Institute of Electrical and Electronics Engineers.

The above document may be obtained from: IEEE Standards Office, 345 East 47th Street, New York, N.Y. l00l7.

Electronic Industries Association

Interface between Data Terminal Equipment and Data Communication Equipment Employing Serial Binary Data Interchange, EIA-232C.

American National Standards Institute

1. 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.

2. Integrated Services Digital Network - Basic Access Interface at S and T Reference Points - Layer 1 Specification, ANS T1.605-1988.

3. Carrier to Customer Installation - DS1 Metallic Interface, ANS T1. 403-1989.

International Organization for Standardization

1. Information Processing Systems - Open Systems Interconnection - Basic Reference Model, Ref. No. ISO 7498-1984(E).

2. Information Processing Systems - Data Communications - Use of X.25 to provide the OSI Connection Mode Network Service, IS 8878.

3. Information Processing Systems - Open Systems Interconnection - Network Service Definition, IS 8348.

4. Information Processing Systems - Open Systems Interconnection - Addendum to the Network Service Definition Covering Connectionless Data Transmission, ISO 8348 Addendum 1.

5. Information Processing Systems - Open Systems Interconnection - Addendum to the Network Service Definition Covering Network Layer Addressing, ISO 8348 Addendum 2.

6. Information Processing Systems - Open Systems Interconnection - Internal Organization of the Network Layer, DIS 8648, N3985, Feb., 1986.

7. Information Processing Systems - Open Systems Interconnection - Protocol for Providing the Connectionless Network Service, IS 8473, N3998, March, 1986.

8. Information Processing Systems - Open Systems Interconnection - Data Communication - X.25 Packet Level Protocol for Data Terminal Equipment, ISO 8208.

9. 7-bit Coded Character Set for Information Processing Interchange, ISO 646, l973.

10. Information Interchange -- Representation of Local Time Differentials, ISO 3307, l975.

11. Information Processing Systems - Open Systems Interconnection - Working Draft - End System to Intermediate System Routing Exchange Protocol for use in Conjunction with ISO 8473.

12. Information Processing Systems - Open Systems Interconnection - Transport Service Definition, ISO 8072, l984.

13. Information Processing Systems - Open Systems Interconnection - Transport Protocol Specification, ISO 8073, l984.

14. Information Processing Systems - Open Systems Interconnection - Session Service Definition, ISO 8326, l987(E).

15. Information Processing Systems - Open Systems Interconnection - Session Protocol Specification, ISO 8327, I987(E).

16. Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management Part 1: General Introduction, ISO 8571-1.

17. Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management Part 2: The Virtual Filestore Definition, ISO 8571-2.

18. Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management Part 3: File Service Definition, ISO 8571-3.

19. Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management Part 4: File Protocol Specification, ISO 8571-4.

20. Information Processing Systems - Open Systems Interconnection - Connection-Oriented Presentation Service Definition, ISO 8822.

21. Information Processing Systems - Open Systems Interconnection - Connection-Oriented Presentation Protocol Specification, ISO 8823.

22. Information Processing Systems - Open Systems Interconnection - Service Definition for Association Control Service Element - Part 2: Association Control, ISO 8649.

23. Information Processing Systems - Open Systems Interconnection - Protocol Specification for Association Control Service Element: Association Control, ISO 8650.

24. Information Processing Systems - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1), ISO 8824.

25. Information Processing Systems - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1), ISO 8825.

26. Information Processing Systems - Data Communications - High-Level Data Link Control Procedures - Description of the X.25 LAPB-compatible DTE Data Link Procedures, ISO 7776.

27. Information Processing Systems - Data Interchange - Structures for the Identification of Organizations, ISO 6523, 1984.

28. Information Processing Systems - Local Area Networks - Part 2: Logical Link Control, DIS 8802/2.

29. Information Processing Systems - Local Area Networks - Part 3: Carrier Sense Multiple Access With Collision Detection, ISO 8802/3

30. Information Processing Systems - Local Area Networks - Part 4: Token-passing Bus Success Method and Physical Layer Specifications, ISO 8802/4.

3l. Information Processing Systems - Local Area Networks Part 5: Token Ring Access Method and Physical Layer Specifications, ISO 8802/5.

32. Information Processing Systems - Open Systems Interconnection - Virtual Terminal Services - Basic Class, ISO 9040.

33. Information Processing Systems - Open Systems Interconnection - Virtual Terminal Protocol - Basic Class, ISO 9041.

34. Information Processing Systems - Open Systems Interconnection. Virtual Terminal Service, Basic Class, ISO 9040, Addendum 1, 1988.

35. Information Processing Systems - Open Systems Interconnection, Virtual Terminal Protocol, Basic Class, ISO 9041, Addendum 1, 1988.

36. Information Processing - Text and Office Systems-Office-Document Architecture (ODA) and Interchange Format - Part 1: Introduction and General Principles, ISO 8613-1, 1988.

37. Information Processing - Text and Office Systems-Office-Document Architecture (ODA) and Interchange Format - Part 2: Document Structures ISO 8613-2, 1988.

38. Information Processing - Text and Office Systems-Office-Document Architecture (ODA) and Interchange Format - Part 4: Document Profile, ISO 8613-4, 1988.

39. Information Processing - Text and Office Systems-Office-Document Architecture (ODA) and Interchange Format - Part 5: Office Document Interchange Format (ODIF), ISO 8613-5, 1988.

40. Information Processing - Text and Office Systems-Office-Document Architecture (ODA) and Interchange Format - Part 6: Character Content Architectures, ISO 8613-6, 1988.

41. Information Processing - Text and Office Systems-Office-Document Architecture (ODA) and Interchange Format - Part 7: Raster Graphics Content Architectures, ISO 8613-7, 1988.

42. Information Processing - Text and Office Systems-Office-Document Architecture (ODA) and Interchange Format - Part 8: Geometric Graphics Content Architectures, ISO 8613-8, 1988.

43. Information Processing Systems - Protocol Identification in the Network Layer, DTR 9577.

44. Information Processing Systems - End System to Intermediate System Routing Exchange Protocol for use with ISO 8473, IS 9542.

45. Information Processing Systems - Data Communications - Provision of the OSI Connection-mode Network Service, by Packet Mode Terminal Equipment connected to an Integrated Services Digital Network (ISDN), DIS 9574.

46. Information Processing Systems - Transport Service Definition covering Connectionless Mode Transmission, ISO 8072/ADD.

47. Information Processing Systems - Protocol for Providing the Connectionless Mode Transport Service, ISO 8602.

48. Information Processing Systems - Telecommunications and information exchange between systems - OSI Routing Framework, ISO/TR 9575.

49. Information Processing Systems Telecommunications and information exchange between systems - Intermediate systems to Intermediate system Intra-Domain routing exchange protocol for use in conjunction with the protocol for providing the Connectionless mode Network Service ISO/IEC JTC1/SC6 DP 10589.

The above documents may be obtained from:

ANSI Sales Department
1430 Broadway
New York, NY 10018
(212) 642-4900

International Telephone and Telegraph Consultative Committee

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.40l, (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.4l0, (Red Book, 1984), Message Handling Systems: Remote Operations and Reliable Transfer Server.

7. CCITT Recommendation X.4ll, (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.214, (Red Book, 1984), Transport Service Definition for Open Systems Interconnection for CCITT Applications.

11. CCITT Recommendation X.224, (Red Book, 1984), Transport Protocol Specification for Open Systems Interconnection for CCITT Applications.

12. CCITT Recommendation X.215 (Red Book, 1984), Session Service Definition for Open Systems Interconnection for CCITT Applications.

13. CCITT Recommendation X.225 (Red Book, 1984), Session Protocol Specification for Open Systems Interconnection for CCITT Applications.

14. CCITT Recommendation X.400 - Series Implementor's Guide (Version 6, November 1987).

15. CCITT Recommendation X.121 (Red Book, 1985), International Numbering Plan for Public Data Networks.

16. CCITT Recommendation V.35 - Data Transmission at 48 kilobits/second using 60-108 kHz group band circuits.

17. CCITT Recommendation T.410 (Blue Book, 1988) Open Document Architecture (ODA) and Interchange Format - Overview

18. CCITT Recommendation T.411 (Blue Book, 1988) Open Document Architecture (ODA) and Interchange Format - Introduction and General Principles

19. CCITT Recommendation T.412 (Blue Book, 1988) Open Document Architecture (ODA) and Interchange Format - Document Structures

20. CCITT Recommendation T.414 (Blue Book, 1988) Open Document Architecture (ODA) and Interchange Format - Document Profile

21. CCITT Recommendation T.415 (Blue Book, 1988) Open Document Architecture (ODA) and Interchange Format - Document Interchange Format (ODIF)

22. CCITT Recommendation T.416 (Blue Book, 1988) Open Document Architecture (ODA) and Interchange Format - Character Content Architectures

23. CCITT Recommendation T.417 (Blue Book, 1988) Open Document Architecture (ODA) and Interchange Format - Raster Graphics Content Architectures.

24. CCITT Recommendation T.418 (Blue Book, 1988) Open Document Architecture (ODA) and Interchange Format - Geometric Graphics Content Architectures.

25. CCITT Recommendation Q.921 (I.441) (Blue Book, 1988) ISDN User-Network Interface Data Link Layer Specification.

26. CCITT Recommendation Q.931 (I.451) (Blue Book, 1988) ISDN User-Network Interface Layer 3 Specification for Basic Call Control.

27. 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 l2ll, Geneve 20 SWITZERLAND.

Miscellaneous

1. Manufacturing Automation Protocol

2. Technical and Office Protocols, Specification Version 3.0

For copies of the two documents listed above, contact: Corporation for Open Systems, 1750 Old Meadow Road, McLean, VA 22102-4306.

FOREWORD TO THE APPENDICES

Appendices 1-5 describe U. S. Government advanced requirements for which adequate specifications have yet to be developed. This section, revised by the GOSIP Advanced Requirements Group, gives an updated and more complete summary of protocols planned for inclusion in future versions of the document. Each summary states the requirements for including the protocol in GOSIP and a plan of work to meet those requirements.

New versions of GOSIP will be issued no more frequently than once a year and the comments of manufacturers, government agencies and the public will be solicited before each new version is released.

The following protocols are candidates for inclusion in Version 3 of GOSIP.

1. Directory Services
2. Optional Class 2 Transport Protocol
3. CGM
4. Virtual Terminal (X3, page, scroll profiles)
5. MHS extensions based on 1988 CCITT Recommendations
6. FTAM extensions
7. FDDI
8. Network Management (Also the subject of a separate FIPS.)
9. Optional Security Enhancements
10. SGML
11. Manufacturing Message Specification
12. Intra-domain Dynamic Routing
13. EDI

The following protocols are candidates for inclusion in Version 4 of GOSIP.

1. Transaction Processing
2. Remote Database Access
3. Additional Optional Security Enhancements
4. Additional Network Management Functions
5. Inter-domain Dynamic Routing

The purpose of Appendices 1-5 is to assist federal agencies in planning decisions relating to the acquisition of implementations of OSI protocols.

Appendix 6 specifies a list of acronyms.

These appendices are not part of the Federal Information Processing Standard.

APPENDIX 1. SECURITY

1.1 BACKGROUND

The Open Systems Interconnection Security Architecture is now an International Standard (IS 7498/2). This document provides a general architecture that may be used in implementing security services in OSI networks. Five primary security services are specified in the architecture as well as the OSI layers at which security services could be offered. The document also discusses many security mechanisms which can be used in providing the services.

The OSI Security Architecture provides a basis for developing security but it does not provide specifications for implementing security. A significant level of effort is required before specifications for security are available that can be used in standards. This appendix addresses the need for security standards, the status of standards being developed and plans for developing additional required standards.

While the term "Open Systems" implies that users of such systems intend that the systems be open to others, the users always want to provide access to such systems only to authorized users for authorized purposes. Systems that process sensitive and valuable data, especially classified data, must be protected from a wide variety of threats. Vulnerabilities of open systems include unauthorized access and denial of service. Vulnerabilities of data in open systems include unauthorized disclosure, modification and destruction, both accidentally and intentionally.

Computer programs designed to obtain, modify or destroy data or to simply deny service to authorized users are a threat to networks of computers. Such a program is often called a Virus or a Worm. Computers which allow programs to be executed that have been imported from an external source, either via the network or through a storage medium, may be vulnerable to such programs. Users should always have back-up copies of valuable data in an off-line storage facility in case the on-line data is modified or destroyed. Trusted systems with isolation and controlled sharing mechanisms should be used to minimize the threat of a Virus or a Worm.

Security is an option in GOSIP. As such, security services may be provided at one or more of the layers 2, 3, 4, 6 and 7. The Appendix 1 figure depicts placement of security in the overall profile by augmenting Figure 3.2 with optional security in order to form the Government OSI security architecture. The security architecture described here suggests a range of choices for security services and their placement. It is expected that a subset of these services and layers will adequately satisfy specific security requirements. Because security inherently restricts access and if applied at different layers will prohibit interoperability, it is the responsibility of an acquisition authority to insure that the security options chosen provide the desired interoperability as well as the required security.

1.2 REQUIREMENTS

The primary security services that are defined in the OSI security architecture are authentication, access control, confidentiality, integrity and non-repudiation. These are defined in detail in IS 7498/2 and are summarized, with simple examples given, below:

*Data confidentiality services protect against unauthorized disclosure. Protecting the details of an attempted corporate takeover is an example of the need for confidentiality.

*Data integrity services protect against unauthorized modification, insertion and deletion. Electronic funds transfer between banks requires protection against modification of the information.

*Authentication services verify the identity of communicating peer entities and the source of data. Owners of bank accounts require assurance that money will be withdrawn only by the owner.

*Access control services allow only authorized communication and system access. Only financial officers are authorized access to a company's financial plans.

*Non-repudiation with proof of origin provides to the recipient proof of the origin of data and protects against any attempt by the originator to falsely deny sending the data or its contents. Non-repudiation with proof of origin can be used to prove to a judge that a person signed a contract.

Requirements have been identified for government applications for all five of these services, especially the first four. Authentication, confidentiality and integrity services may be implemented in layers 3, 4 and 7 of the OSI architecture while access control and non-repudiation services are offered only at layer 7. Applications, such as Electronic Message Handling Systems, can be provided all security services at layer 7. Providing security at either layer 3 or 4 is generally required but not at both layers. The selection of security services at specific layers must be made by the acquisition authority and depend on the benefits derived and the costs encountered.

1.3 STATUS

Interoperability standards are required for security at layers 2, 3, 4, and 7 of the OSI architecture. Specifications for security at layers 3 and 4 as well as for Electronic Message Handling Systems have been prepared within the Secure Data Network System project. (See NISTIR 90-4250) Specifications for security at layer 2 are being drafted by the IEEE 802.10 LAN Security Working Group developing a Standard for Interoperable LAN Security (SILS). Specifications for authentication of data have been issued in standards by the National Institute of Standards and Technology (formerly the National Bureau of Standards) (FIPS 113) and ANSI (ANSI X9.9). Specifications for key management protocols have been issued in a standard by ANSI (X9.17).

The OSI Implementors' Workshop Special Interest Group in Security is reviewing the specifications of SDNS (See NISTIRs 90-4259 and 90-4262) as they become public. It is also reviewing proposals on security management. It has reviewed several security frameworks and architectures that may be used for future security standards development.

1.4 PLANS FOR ACHIEVEMENT

The specifications and standards referenced above will be reviewed by the security staff of NIST, by the members of the OSI Implementors Workshop Security SIG and by members of the GOSIP committee for inclusion in one or more of the following: Federal Information Processing Standards; ANSI Standards; and ISO Standards. The following outlines the plans for satisfying the requirements for security in OSI, the development of public specifications and the development of standards incorporating the specifications.

1.4.1 OSI Security Architecture

The OSI Security Architecture (IS 7498/2) was adopted as an International Standard in 1988. This document is included in the Implementors Agreements as being the basis for all OSI security development. No further work is needed on this document at this time.

1.4.2 OSI Security Frameworks

A set of security frameworks of specific information processing applications are planned by the ISO/IEC/JTC 1/SC21/WG1 Security Group. An authentication framework is an example of such a framework. The Security SIG will continue to review these frameworks for adoption in the Implementors Agreements or to develop frameworks that are needed but are not in development in ISO.

1.4.3 Data Link Layer Security

An IEEE Standard for Interoperable LAN Security is being developed over the next 1-2 years by the IEEE 802.10 LAN Security Working Group. A Standard for Interoperable LAN Security could be ready in 1990 for consideration by the OSI Implementors Workshop Security SIG.

1.4.4 Network Layer Security

The SDNS Network Layer Security protocol document (SP3) is available for public use. This protocol was presented to ANSI in 1989. The protocol encapsulates the T-PDUs just like the Transport Layer security protocol except that it can also add network addresses to the protocol header for network routing. The protocol may be implemented in intermediate gateway systems as well as end systems. A Network Layer Security protocol standard could be ready in 1991.

1.4.5 Transport Layer Security

The SDNS Transport Layer Security protocol document (SP4) is available for public use and a FIPS is being proposed based on this work. This protocol was presented to ANSI and ISO in 1989. The protocol encapsulates the Transport Protocol Data Units, adds an integrity code if integrity is desired, encrypts the entire T-PDU if confidentiality is desired, and then puts the result in a SE T-PDU (SE stands for security envelope or secure encapsulation). A receiver that has the correct cryptographic key can decrypt the SE T-PDU, verify its integrity and then process the resulting T-PDU. A Transport Layer Security protocol standard could be ready in 1991.

1.4.6 Electronic Message Handling System Security

The X.400 Electronic Message Handling System security recommendations and the DARPA Mail Security RFC 1040 are available for public use. The SDNS Message Handling Security protocol specifications are also available for public use. A standard format for secure electronic messages could be ready in 1992.

1.4.7 Cryptographic Key Management Protocols

The ANSI X9.17 Key Management Protocol, which is based on private key cryptographic algorithms, and several public key management protocols are being reviewed by the NIST security staff. A key management protocol based on public key cryptographic algorithms could be ready in 1993 for implementation.

Figure A.1 Framework for OSI Security

APPENDIX 2. SYSTEM AND ARCHITECTURE

2.1 Network Management

OSI management functionality supports the location and correction of faults, the establishment and adjustment of configurations, the measurement and tuning of performance, the management of security, and collection and reporting of billing and accounting information. Such functionality is in end systems (hosts), intermediate systems (routers), and other network elements (e.g., network services, bridges, switches, modems, and multiplexors). The primary goal for a Federal Government network management specification is to create the ability for managing multi-vendor computer and telecommunications networks remotely without undue use of proprietary management protocols. The scope of a network management specification for use by the U.S. Government will include protocols for exchanging management information and the definition and format of information to be exchanged.

Note: The primary vehicle for this specification will be a Federal Information Processing Standard (FIPS). This FIPS will reference GOSIP and will be referenced by GOSIP. (The FIPS is discussed further below under "Plan".)

Requirements

Requirements for OSI network management are described in detail within a NIST report, Management of Networks Based on Open Systems Interconnection (OSI) Standards: Functional Requirements and Analysis (NIST Special Publication 500-175, November 1989). Requirements exist for an overall management architectural framework model including fault, accounting, configuration, security, and performance management services.

Status

The OSI management standards are in an intermediate stage of their development and are progressing rapidly. Key areas for management standards are architecture, protocols, system management functions, and the structure of management information. The following table lists the latest available ISO schedule for management standards approved at the Sixth SC 21/WG 4 Meeting in Florence, October 31 - November 9, 1989.

	TARGET DATES		
	DP	DIS	IS
Management Architecture			
Management Framework	9/86	6/87	10/88
Systems Management Overview			7/90
4/91			
Management Protocol			
Common Management Information Service			1/90
Addendum 1: CancelGet		9/89	7/90
Addendum 2: Add/Remove		9/89	7/90
Common Management Information Protocol			1/90
Addendum 1: CancelGet		9/89	7/90
Addendum 2: Add/Remove			9/89
7/90			
Structure of Management Information			

Part 1: Management Information Model		5/89	1/90
1/91			
Part 2: Definition of Management Information		7/90	4/91
Part 4: Guidelines for the Definition of Managed Objects	11/89	1/91	1/92

TARGET DATES

	DP	DIS	IS
Management Functions			
Configuration Management			
Systems Management - Part 1:			7/90
7/91			
Object Management Function			
Systems Management - Part 2:		7/90	7/91
State Management Function			
Systems Management - Part 3:			7/90
7/91			
Relationship Management Function			
Fault Management			
Systems Management - Part 4:			7/90
7/91			
Alarm Reporting Function			
Systems Management - Part 5:			7/90
7/91			
Event Report Management Function			
Systems Management - Part *:		7/90	4/91
4/92			
Confidence and Diagnostic Testing Function			
Systems Management - Part 6:		11/89	7/90
7/91			
Log Control Function			
Security Management			
Systems Management - Part 7:	11/89	7/90	7/91
Security Alarm Reporting Function			
Systems Management - Part *:	7/90	4/91	4/92
Security Audit Trail Function			
Accounting Management			
Systems Management - Part *:	7/90	4/91	4/92
Accounting Metering Function			
Performance Management			
Systems Management - Part *:	7/90	4/91	4/92
Workload Monitoring Function			
Systems Management - Part *:		7/90	4/91
4/92			
Measurement Summarization Function			

As can be seen from the above schedule, there are several important standards that have now reached, or soon will reach, International Standard (IS) status. However, many others are still two years away from IS. Still others that are planned, e.g., Software Management (including "down-line load"), have not yet been added to the schedule. It is important to note that the Draft International Standards (DISs) scheduled to be available by the end of 1990 comprise a subset that will make it possible for vendors to build useful systems to solve many immediate network management problems.

Standards for the specification of managed objects are now being developed by ISO, ANSI, CCITT, and the IEEE, as well as by the Internet Engineering Task Force of the Internet Activities Board (for management of TCP/IP oriented networks). In general, full specifications and standards from these organizations are expected to lag the above SC21/WG4 management schedule by more than a year.

Another important aspect of network management standards activity is the development of implementation agreements (IAs). The network management SIG of the NIST OIW is developing IAs based upon the emerging network management standards. These agreements are being developed according to a phased approach that aligns with the ISO standards as they progress from DP to IS. The OSI/NM Forum is also developing a set of agreements (termed specifications) for network management. These agreements, based on earlier ISO documents and original Forum work, are to be used as a basis for Forum-sponsored interoperable management demonstrations planned for 1990 and beyond. Both formal and informal liaison between the NMSIG of the OIW and the NM Forum has proved mutually beneficial in advancing each set of agreements, including identifying and correcting errors and omissions.

Plan

There is an urgent need today for products to manage multi-vendor computer and telecommunications networks. The U.S. Government requires initial network management specifications that provide a useful subset of the full OSI management functionality. It is desirable to specify the initial subset in such a way that it is easy to add other capabilities to reach the full set of management functionality. Such additional functionality may include the management of future technologies such as ISDN and FDDI, and may include new management services such as software management and time management.

The U.S. Government intends to propose an initial FIPS based on the OIW stable network management IAs. The OIW will include at most the following in its agreements to be completed in 1990 (from phase one of the OIW IAs):

Management Functions:
Object Management, State Management, Relationship Management, Error Reporting and Event Control

Management Information:
Information Model, Naming, Guidelines and Template for Defining Managed Objects

Management Communication:
CMIS/P, Association Policies, and Services Required

Management Objects:
Support Objects required for above and selected Managed Object Definitions under development by the OSI MIB WG

Conformance Criteria:
TBD depending on the progress of relevant ISO documents.

It is planned that the initial network management FIPS will be based on portions of the above phase one stable agreements. The FIPS will include specifications for a management protocol based on OIW IAs for CMIS/CMIP, and it will include management function specifications based on the OIW IAs. Also, the FIPS will include a library of management objects (MIL). In addition, other portions of the agreements may be cited in the FIPS.

GOSIP profiles will be cited in the FIPS to specify the protocol stack upon which management information will be conveyed and to include OSI applications suitable to support management of networks.

Once an initial management FIPS has been established, portions of future GOSIP versions may reference management FIPS as appropriate. For example, to specify management of network end system (host) computers, GOSIP might reference the Network Management FIPS sections on the use of CMIS/CMIP as a method for conveying information and sections on system management functions for specific management services. GOSIP might also reference the management FIPS for appropriate managed object definitions. Likewise for the management of network routers, GOSIP might reference the FIPS for use of CMIS/CMIP, management functions and managed object definitions.

These are possible initial examples. As both the FIPS and GOSIP mature, GOSIP will likely make many additional references to newer versions of the management FIPS. (And the FIPS can be expected to additionally reference newer versions of GOSIP as well.)

2.2 REGISTRATION

OSI Registration procedures are the key to creating globally unique identifiers for OSI objects. Most OSI objects are identified via a hierarchically structured label. Specific procedures must be established to ensure that GOSIP identifiers fit within an internationally recognized plan and uniquely identify GOSIP objects.

Requirement

Procedures are required for the registration of OSI objects, such as organization numbers and names. The specific complete list of objects is subject to further study and is likely to evolve over time, as directory services are adopted. For the first version of GOSIP, procedures were required for registration of organization identifiers for use in NSAPs, labels for electronic mail private body parts, and organization names for electronic mail addresses. The third version of GOSIP will require extending the procedures to include directory distinguished names. An immediate requirement not specific to GOSIP is registration procedures for objects defined in the OSI Implementor's Agreements.

Status

A standard for registration procedures is under development in ISO. The NIST is already maintaining a small registration service for OSINET members. The NIST has secured three international code designators (ICDs) as follows: 1) four (4) allocated to OSINET and the NIST/OSI Implementor's Workshop; 2) five (5) allocated to the U. S. Government, and 3) fourteen (14) allocated to the OSI Implementors' Workshop (OIW).

Plan

The NIST is updating the GOSIP User's Guide for publication with Version 2 of GOSIP. One section of the guide will detail GOSIP registration procedures. A registration SIG in the NIST OSI Implementors' Workshop has identified objects requiring registration and established detailed procedures for registering the objects.

2.3 ADDRESSING

GOSIP network addressing is limited to defining NSAPs. The existing assumption is that NSAPs will be retrievable from a directory service and that each NSAP will address a single host. Nothing within GOSIP is designed to preclude multi-homed or mobile end systems. The problem is that no routing protocol exists to deal with mobile hosts at the speed required for some applications. At the present time, there is no definition for the semantics and syntax of multi-cast addressing within the network layer.

Requirement

Multi-cast addressing is required to support operation on broadcast networks with connectionless protocols.

Status

No work is underway in this area.

Plan

Study inclusion of multi-cast NSAPs for operation over broadcast networks (e.g., local networks) in conjunction with connectionless transport, network, and data link protocols.

APPENDIX 3. UPPER LAYERS

3.1 X.400 EXTENSIONS

Message Handling System specifications in Version 2 of GOSIP are based on the 1984 CCITT Recommendations. GOSIP MHS extensions will be based on the CCITT 1988 Recommendations. These recommendations provide new capabilities including security, delivery to a physical delivery service, use of a directory service, delivery to a message store, and an OSI architecture which includes ACSE and the Presentation layer.

Requirements

A requirement exists for MHS security features such as message originator authentication, checks against unauthorized disclosure and verification of content integrity. It is also highly desirable to have message store delivery which will allow personal computers without full User Agent functionality to have access to MHS services. The DOD requires that military precedence levels and preemption features be incorporated into the Message Handling Systems standard and that a method be developed of passing this information to the connectionless network layer protocol for processing.

Status

A. Standards - The 1988 CCITT MHS Recommendations were formally approved in late 1988.

B. Implementors' Agreements - In 1989, the MHS SIG issued implementors' agreements which provided a minimally conformant 1988 Message Handling System. These implementors' agreements do not include significant additional user services, but allow interworking with implementations conforming to the NIST Stable Implementation Agreements for CCITT 1984 X.400-based Message Handling Systems and provide a firm basis for the introduction of further 1988 services and features. Further implementors' agreements based on CCITT 1988 X.400 are expected in 1990.

Plan

As an interim measure, NSA and NIST should determine whether the SDNS method of sending security information in a new special-purpose User Agent satisfies all GOSIP advanced security requirements for electronic mail. This approach would allow security information to be sent on Message Handling Systems implemented according to the CCITT 1984 Recommendations. However, the new User Agent would not be based on an international standard.

There already exists the capability of sending and receiving X.400 mail from a personal computer attached to a host by using terminal emulation software. The User Agent is co-located with the MTA and the terminal interface is a local matter. The GOSIP Advanced Requirements Group plans to investigate to what extent this architecture satisfies current government requirements.

There is also a proposal to include a message store (i.e., standard remote User Agent) capability in a future MHS implementors' agreement. A message store would provide a standard software package with standard error recovery. When implementors' agreements for message store are adopted, the functionality in those agreements will be incorporated into GOSIP.

The DoD requirement for expansion of precedence levels will be forwarded to the CCITT committee on Message Handling Systems. The GOSIP Advanced Requirements Group will request the

NIST/OSI Implementors' Workshop to determine how Application-level precedents can be passed to the lower layers for processing.

3.2 FTAM (FILE TRANSFER, ACCESS AND MANAGEMENT)

The File Transfer, Access and Management protocol and service allow users on different networks to communicate about files (and transfer files) without requiring that one user know the detailed file characteristics of the other user. A generic file organization is defined for communication; elements of this virtual file model are mapped to corresponding elements of the local file system. A comprehensive set of file attributes and file activity attributes are defined; in addition, a large number of actions is possible on a wide variety of file types.

Requirement

Implementation profiles are defined for user requirements as follows: simple file transfer, positional file transfer, full file transfer, simple file access, full file access, and management. Each implementation profile contains a different combination of document types, attributes and service classes. An FTAM implementation for the GOSIP should require support of the positional file transfer (which includes simple file transfer), simple file access and management implementation profiles. Future versions of GOSIP should include overlapped access, filestore management (including file directory query capability), error recovery capability, concurrency control capability, and File Access Data Unit (FADU) locking capability.

Status

A. Standards - FTAM has been released as an International Standard from ISO; currently FTAM comprises five parts: general introduction, virtual filestore definition, file service definition, file protocol specification, and protocol information conformance statement proforma. There are two prospective addenda which are overlapped access and filestore management. Filestore management should reach IS status in late 1991, and overlapped access should reach IS status in early 1992.

B. Implementors' Agreements - FTAM Phase 2 (based on IS text) was completed as of December 1988, and maintained since then with the inclusion of several errata. This agreement provides for all core services defined in the FTAM standard except for restart, recovery and concurrency. Facilities for full file transfer and record-level access are provided; three different FTAM, and four different NIST document types are defined. FTAM Phase 2 is included in Version 3 of the workshop agreements, available after December 1989. FTAM Phase 3 provides restart, recovery and concurrency capabilities, and enlarges on the set of document types currently defined. FTAM Phase 3 is complete as of March 1990. FTAM Phase 2 Agreements are upwardly compatible to FTAM Phase 3 Agreements at the intersection of their functional capabilities.

Plan

FTAM Phase 2 is currently included in versions 1 and 2 of GOSIP; reference is made to the Phase 2 FTAM (based on IS) as it appears in the workshop agreements. A file directory service capability is planned for in a future version of GOSIP; it is also anticipated that a number of new document types will be included in the future. Possibly, full file transfer and full file access implementation profiles will be mandated. Recovery, restart and concurrency control capabilities may also be required. It is anticipated that Version 3 of GOSIP will mandate the FTAM Phase 3 specification from the Workshop Agreements. NIST personnel will work with the FTAM Special Interest Group at the NIST/OSI Implementors' Workshop to expedite the development of implementation agreements and to insure that government requirements are included.

3.3 VIRTUAL TERMINAL

The Basic Class Virtual Terminal Protocol allows terminals and hosts on different networks to communicate without requiring that one side know the terminal characteristics handled by 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.

Requirement

The service options to be selected include type of negotiation and the VT profiles to be specified. Additional implementation profiles for GOSIP will include profiles for page and scroll terminals in addition to the existing TELNET and forms profiles. No negotiation capability is required.

Status

A. Standards - All comments on Basic Class VT and on addendum 1 (forms) have been resolved and the service and protocol documents for Basic Class and the addendum have been merged.

B. Implementors' Agreements - Stable agreements were completed for the TELNET, Transparent, and Forms profiles in December 1988. Stable Agreements for the X3 profile were completed in December 1989.

Plan

Version 3 of GOSIP is expected to include the X3, scroll and page profiles. Additional options may be added to the TELNET profile. NIST personnel will work with the VT Special Interest Group in the NIST/OSI Implementors' Workshop to expedite the development of implementation agreements and to insure that government requirements are included.

3.4 THE DIRECTORY

A directory is a collection of attributes (i.e., information) about, and relations between, a named set of addressable objects within a specific context. A directory can be viewed as a data base containing instances of record types. The most typical relationship between a directory user and the directory itself is that of an information user and an information provider. The user supplies an unambiguous or ambiguous key to the directory, and the directory returns the information labeled by the key. The directory user may filter the available information to access only the most essential fields.

Requirement

The requirements for a GOSIP directory service are much too complicated and voluminous to include here. The NIST has developed a separate report specifying the requirements. From the complete requirement set, the NIST has identified an initial subset for inclusion into GOSIP. In summary, for the initial directory, requirements include: 1) functions provided by the DoD "whois" service (a name to data record mapping), and the DoD domain name service (host name to network address mapping), 2) service name to T-selector, S-selector, and P-selector mapping, 3) inclusion of a host's capabilities within the host directory entry, and 4) the ability to resolve mailing list names into a set of electronic mail addresses. For the initial GOSIP directory, access control, simple authentication, and replication are also required.

Status

The Directory is an IS in ISO (ISO 9594) and has been issued by CCITT as the X.500 series of Recommendations. Workshop Agreements exist based on these documents. ISO and CCITT are jointly developing extensions to the current standard in areas where it is known to be deficient, such as access control, replication, and the information model. Additional implementation agreements are needed to cover the extensions.

Plan

The plan is to improve the directory implementor agreements as necessary and to get needed changes into the ISO and X.500 versions of the standard to support the initial GOSIP requirements. These goals should be accomplished in 1991 and 1992 so that an initial directory specification can be included in a subsequent version of GOSIP.

3.5 REMOTE DATABASE ACCESS

Remote Database 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.

Requirement

There is a strong requirement to share information among Database Management Systems from different vendors which are widespread in both government and industry. The Remote Database Access protocol allows that data sharing by providing a neutral "language" by which heterogeneous systems can communicate.

An extension of the above requirement is the need for distributed database capability. This will be achieved in the long-term by extending the existing RDA model, and through RDA's harmonization with the Transaction Processing protocol.

Status

The RDA standard is specified in two documents, a generic RDA for arbitrary database connection and an SQL specialization for connecting databases conforming to the standard database language SQL. Both the generic RDA standard and the RDA specialization for SQL include functionality required by Federal agencies.

The generic RDA standard reached DP status in 1987 and is expected to reach DIS status in 1990. The RDA specialization for SQL is also expected to reach DP status in 1990. Final adoption of ISO International Standards for both documents is expected in 1992.

Plan

Vendors, particularly SQL vendors, plan to have implementations conforming to the ISO International Standard available at the earliest possible time. An RDA SIG was formed within the NIST OSI Implementors' Workshop in 1989 to assist in this process.

3.6 TRANSACTION PROCESSING

Requirement

The specific requirements within the U. S. Government for transaction processing are still under investigation.

Status

Current plans are for Transaction Processing to move to IS status in 1990 or in 1991.

Plan

NIST is working with Federal agencies to determine transaction processing requirements and is representing the interests of Federal agencies in the national and international standards committees. The first step is for the federal agencies that have transaction processing requirements to become knowledgeable about the TP services specified in the evolving TP standards documents and to determine whether these services meet the needs of their organization. NIST is willing to assist other federal agencies in the process.

A Transaction Processing SIG has been formed within the NIST/OSI Implementors' Workshop.

3.7 ELECTRONIC DATA INTERCHANGE

Electronic Data Interchange (EDI) describes the rules and procedures that allow computers to send and receive business information in electronic form. Business information includes the full range of information associated with buyer/seller relationships (e.g., invoices, Customs declarations, shipping notices, purchase orders).

Requirements

The Office of Management and Budget is proposing to issue a guidance document that states that Federal agencies shall, to the maximum extent practicable, make use of Electronic Data Interchange with supporting GOSIP telecommunications networks for the processing of business-related transactions.

Status

A. Standards - 1) ANSI committee X12 has developed and is developing standard formats for business-related messages. There is also an ISO standard (IS 9735) for Electronic Data for Administration, Commerce and Transportation (EDIFACT). The JTC1 special working group on EDI is developing a conceptual model for Electronic Data Interchange. 2) CCITT Study Group VII established a Rapporteur Group to work on a solution on how to perform EDI using Message Handling Systems. The group completed work on a set of recommendations in June 1990. This group established a new content type for EDI and a corresponding content protocol (currently designated P_{EDI}). P_{EDI} will provide service elements and heading fields for EDI similar to those provided by P2 for interpersonal messages.

B. Implementors' Agreements - The NIST Workshop Agreements currently contains basic guidelines for adopting 1984 X.400 as the interim data transfer mechanism between EDI applications.

Plan

If products based on the CCITT Interim Recommendations are available in 1992, EDI will be included in Version 3 of GOSIP; Otherwise, EDI is scheduled for inclusion in Version 4 of GOSIP.

3.8 MMS SERVICES

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.

Requirements

Although the government is not a primary manufacturer, MMS has usefulness in the acquisition of point of measurement quality data, in military depots at the Department of Energy, and Department of Defense sites. Additionally, the Deep Space Network Data Systems group of the Jet Propulsion Laboratory is investigating the use of MMS for on-board control and telemetry.

Status

MMS is currently at the IS level in ISO and has implementors' agreements ready for inclusion in the NIST/OSI Stable Implementor Agreements in 1990.

There are implementations available based upon DIS-9506(MMS) which are already installed. A mechanism for backwards compatibility has been agreed and is ready to progress into the Stable Agreements document. Work is ongoing to establish agreements on all 86 services that are contained within MMS.

Plan

The plan is to augment and improve the MMS implementors' agreements as required. Additionally, abstract test cases will be reviewed and generated as necessary to further refine the definition of MMS conformance. This work is ongoing with anticipated completion of a subset of services in 1990 so that MMS can be included in Version 3 of GOSIP.

3.9 INFORMATION RETRIEVAL

Information retrieval supports the open interconnection of database users with database providers by specifying an OSI application layer protocol for intersystem search and retrieval of records from a remote bibliographic database.

Requirement

Information retrieval functionality is required by Federal agencies which need to retrieve information from remote bibliographic databases.

Status

The OSI Information Retrieval service and protocol is specified in the ANSI standard: Z39.50-1988 - *Information Retrieval Service Definition and Protocols Specification for Library Applications.* A corresponding ISO standard (ISO 10162 and 10163: Search and Retrieve Service Definition and Protocol Specification) has reached DIS status. Final adoption as international standards is expected by early 1991.

Plan

Vendors are now developing implementations conforming to Z39.50. A Z39.50 implementor's group has been formed, represented by more than 20 companies. Options will be investigated to include bibliographic searching within GOSIP. Agencies are encouraged to bring forth other information retrieval requirements.

APPENDIX 4. EXCHANGE FORMATS

The following standards are not OSI standards, but they provide services required by Federal agencies and the format information that they specify can be transferred by OSI Application layer protocols, such as FTAM and MHS.

4.1 ODA EXTENSIONS

ODA allows for the interchange of compound documents (documents containing text, facsimile, and graphics) which have been generated by diverse types of office products, including word processors and desktop publishing systems. Interchange of ODA documents may be by means of data communications or the exchange of storage media. ODA documents may be in processable form (to allow further processing such as editing or reformatting) or in final form (to allow presentation as intended by the originator) or in both forms. The key concept in the document architecture is that of structure -- the division and repeated subdivision of the content of a document into increasingly smaller parts called objects. Two structures are defined by ODA: these are logical structure (contents are divided based on meaning, e.g., chapters, sections, paragraphs) and layout structure (contents are divided based on form, e.g., pages, blocks).

Requirement

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 document. As extensions to ODA are made, they will be incorporated into the DAPs specified in the Workshop Agreements.

Status

A. Standards - ODA is an international standard; however, several areas within ODA are currently being studied, enhanced and/or extended. The primary emphasis on extensions includes new content architectures (such as spreadsheets and audio) and new features such as variant of styles, complex tables, alternative representation, computed data in documents, and an interface to EDI. Several addenda are planned to cover these extensions.

B. Implementors' Agreements - The ODA SIG will examine extensions as they are developed to determine whether or not to incorporate such extensions in DAPs.

Plan

The plan is to contribute to the work on extensions to ODA through the Workshop by informing standards groups of deficiencies and inadequacies of the standard and to incorporate developed extensions into applicable DAPs when these extensions are mature. GOSIP will reference applicable DAPs which the National Computer Systems Laboratory (NCSL) plans to issue for Federal agency use.

4.2 GRAPHICS

The graphics requirements for GOSIP include the Computer Graphics Metafile (CGM). The purpose of CGM is to facilitate the transfer of picture description information between different graphical software systems, different graphical devices and different computer graphics installations. CGM specifies a file format suitable for the description, storage and communication of picture description information in a device-independent manner.

Requirement

FIPS PUB 128 announces the adoption of the American National Standard for Computer Graphics Metafile, ANSI X3.122-1986, as a Federal Information Processing Standard (FIPS). This standard is intended for use in computer graphics applications that are either developed or acquired for government use. When computer graphics metafile systems for GOSIP are developed internally, acquired as part of an ADP system procurement, acquired by separate procurement, used under an ADP leasing arrangement, or specified for use in contracts for programming services, they shall conform to FIPS PUB 128.

Status

A. Standards - Computer Graphics Metafile (CGM) ANSI X3.122-1985, ISO 8632/1-4-1987, FIPS
128-1987.

B. Application Profiles - MIL-D-28003 "Digital Representation of Communication of Illustration Data: CGM Application Profile" 30 December 1988.

Plan

An Application Profile (AP) defines additional requirements beyond ANSI CGM to ensure interoperability of implementations for specific applications. Currently, two major application profiles exist for CGM; the TOP AP, and the CALS AP (MIL-D-28003). As these APs and other APs which are applicable for Federal agency use are promulgated, they will be incorporated into FIPS 128. GOSIP will reference applicable APs for CGM which NCSL plans to issue for Federal agency use.

4.3 STANDARD GENERALIZED MARKUP LANGUAGE (SGML) APPLICATION PROFILE

Description

The Standard Generalized Markup Language (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. The Standard Generalized Markup Language can be used for documents that are processed by any text processing or word processing system. It will be particularly applicable to:

- documents that are interchanged among systems with differing text processing languages

- documents that are processed in more than one way, even when the procedures use the same text processing language.

Requirement

FIPS PUB 152 announces the adoption of the International Standards Organization Standard Generalized Markup Language (SGML), ISO 8879-1986, as a Federal Information Processing Standard (FIPS). This standard is intended for use in documents that are processed by any text processing systems that are either developed or acquired for government use. When SGML text processing systems for GOSIP are developed internally, acquired as part of an ADP system procurement, acquired by separate procurement, used under an ADP leasing arrangement, or specified for use in contracts for programming services, they shall conform to FIPS PUB 152.

Status

A. Standards - *Information Processing - Text and office systems - Standard Generalized Markup Language (SGML),* ISO 8879-1986 (E),FIPS 152-1988.

B. Application Profiles - MIL-M-28001A, "*Markup Requirements and Generic Style Specification for Electronic Printed Output and Exchange of Text,"* December 1989.

MIL-M-28001A, *"Markup Requirements and Generic Style Specifications for Electronic Printed Output and Exchange of Text,"* established the requirements for the digital data form of page oriented technical military publications. Data prepared in conformance to these requirements will facilitate the automated storage, retrieval, interchange, and processing of technical documents from heterogeneous data sources. MIL-M-28001A requirements include:

- o procedures and symbology for markup of unformatted text in accordance with this specific application of the Standard Generalized Markup Language;

- o SGML compatible codes that will support encoding of a technical publication to specific format requirements applicable to technical manuals;

- o output processing requirements that will format a conforming SGML source file to the style and format requirements of the appropriate Formatting Output Specification Instance (FOSI).

Plan

An Application Profile (AP) defines additional requirements beyond FIPS SGML to ensure interoperability of implementation. MIL-M-28001 is an Application Profile for technical military publications. The plan is to develop an SGML Document Application Profile (SDAP) by extending MIL-M-28001 to be more useful for generic documents and to incorporate the SDAP into FIPS 152. GOSIP will reference applicable SDAPs which NCSL plans to issue for Federal agency use.

APPENDIX 5. LOWER LAYER PROTOCOLS

5.1 IS-IS DYNAMIC ROUTING PROTOCOLS

Within OSI networks, systems of routers (intermediate systems) enable the effective and efficient interconnection of a diverse set of subnetwork types (e.g., CSMA/CD, token ring, token bus, and X.25) into internetworks. Within such an internetwork, messages are sent like postal letters from router to router. At each router a message is examined and the next router is selected. The effect of such a scheme is that each message may follow an independent route. As conditions within the internetwork change (e.g., link, host, and router failures and activations), the possibility exists for messages to reach their destination despite failure of network elements. Such potential can only be achieved if the system of routers exchanges information concerning the state of routes. Protocols for exchanging information concerning varying route conditions are known as dynamic routing protocols. Within OSI standards, dynamic routing protocols are named intermediate system to intermediate system (IS-IS) protocols.

Requirement

Dynamic routing is required within GOSIP to support the needs of several large government internetworks. Two kinds of routing support are required: 1) dynamic routing within an administrative domain, and 2) dynamic routing between administrative domains. Routing requirements within an administrative domain are well understood, and two generally acceptable schemes exist. Routing requirements between administrative domains are not widely agreed upon, although ECMA has produced a technical report.

Status

An intra-domain dynamic routing protocol was submitted to ISO from ASC X3S53.3 in January 1988. The submission is based on DEC's Phase V link state routing. It was discussed at the November ISO SC6/WG2 meeting and was registered as a DP in January 1990.

ECMA developed an inter-domain technical report (TR50), based on an NIST-developed model. It was submitted by ECMA as a liaison to ISO WG2 in May 1989 as the proposed basis for an ISO inter-domain standard.

Plan

The NIST will support the progression of the DEC submission toward an ISO IS through work in standards committees and laboratories. The NIST will also prepare for establishing implementor agreements as the document reaches DIS. The NIST will continue to support development of the inter-domain routing protocol within ECMA, ANSI, and ISO.

The GOSIP will adopt intra-domain dynamic routing protocols as soon as implementor agreements are in place. The projected date is 1991. The adoption of an inter-domain routing protocol for GOSIP should occur one to two years following adoption of an intra-domain protocol.

5.2 FIBER DISTRIBUTED DATA INTERFACE (FDDI)

FDDI is a 100 Mbit/s token ring network utilizing multimode fiber optic media. Three standards, Physical Medium Dependent (PMD), Physical Layer Protocol (PHY), and Medium Access Control (MAC) specify the Physical and Data Link layers of the Open Systems Interconnection Reference Model. A fourth standard, Station Management (SMT) interfaces to the first three layers to control initialization and configuration of the ring, as well as reconfiguration around faults, and will provide management services to higher layer management protocols.

Requirement

MAC, PHY and PMD have a few options which require selection (e.g., 48 bit vs. 16 bit addressing) and a few timers and parameters which require further definition (particularly of their default values) to ensure interoperability in an OSI environment. One class of service (Restricted Token Mode) is inappropriate in an OSI environment.

SMT is more complex, and will probably offer many options, particularly regarding network policies, which will require some selection. In many cases, this will simply mean selecting the default option or policy.

Status

A. Standards - The MAC (X3.139-1987) PHY (X3.148-1988) and PMD (X3.166-1989) standards are approved. SMT is still under development and probably will be forwarded in June 1990 and approved in 1991. Products implementing FDDI are now widely available.

B. Implementors' Agreements - NIST has drafted an implementors' agreement covering MAC, PHY and PMD. This was accepted into the ongoing agreements by the Lower Level SIG and should be incorporated in Version 3.0 of GOSIP. Although products are now starting to appear, SMT is not approved, but is "stable", so work could begin on an implementors' agreement by mid-1990.

Plan

NIST will draft a proposed implementors' agreement covering SMT after SMT is forwarded to approval, which will probably occur in June. The ANSI standard, moreover, will not be completely stable until some time in 1990 or 199l, since the public review usually results in changes. That means that closure on implementors' agreements cannot be reached before some time in 1991 at the earliest. This is not ideal, because there will be significant product shipments in 1990.

Since SMT is largely software, vendors expect to update equipment already shipped before SMT is finalized, by distributing new software (often on ROM chips).

5.3 TRANSPORT PROTOCOL CLASS 2

The transport protocol, class 2, for use over the connection-oriented network service (CONS) is accepted by several OSI profiles (e.g., UK GOSIP). The transport protocol, class 2, is also used with CONS in several U.S. Government applications, where communication is confined to a single logical subnetwork.

Requirement

The transport protocol, class 2, is desired in GOSIP as an optional transport protocol for use with CONS, where communication is confined to a single logical subnetwork. The transport protocol, class 4, operating over the connectionless network service (CLNS), will remain the sole mandatory data transport service for purposes of interoperability among U. S. GOSIP-compliant computer systems. The specification of the transport protocol, class 2, as an option in GOSIP, is intended to enable interoperability among U.S. Government computer systems, when using class 2 transport over CONS. Such specifications would be intended to prevent the spread of non-interoperable class 2 transport implementations within the U. S. Government. The ability to choose the correct transport protocol class for a given instance of communication will require a prior knowledge on the part of the transport connection initiator, until directory services are included in GOSIP.

Status

Although a few U.S. vendors provide implementations of the class 2 transport protocol, the overwhelming majority offer class 4 transport only. The Workshop Agreements endorse class 4 transport for use over

CLNS and CONS, and class 0 transport for use over CONS when direct access to public messaging systems is required.

Plan

Interested government agencies brought the requirement for class 2 transport implementation agreements to the attention of the Lower Layer SIG of the NIST/OSI Implementors' Workshop. Workshop Agreements are now in place, so consideration canbe given to inclusion of an optional class 2 transport capability into GOSIP, Version 3.0.

5.4 INTEGRATED SERVICES DIGITAL NETWORK

Integrated Services Digital Networks (ISDN), supporting integrated voice, data, image, and video are expected to be deployed on a wide scale in ubiquitous public offerings and in private network offerings, as services and as components from which private ISDN networks can be constructed. Initial offerings will be a switched 64 kbps service delivered to a customer's terminal at a basic rate (16 Kbps signaling channel and two 64 KBPS data channels) or a primary rate (24 64 Kbps channels, one used for signalling). Later offerings, now in the development phases, will offer higher capacities, estimated at 150 Mbps to 622 Mbps.

Requirement

One use for ISDN is to provide a bearer service for OSI data protocols; thus, ISDN is included in GOSIP as a lower layer service. Other ISDN applications include integrated voice, image, data, and video, and, therefore, non-GOSIP ISDN applications can be expected. NIST plans to issue a variety of FIPS that enable the government to exploit the full technical capabilities of ISDN. The initial focus aims at switched 64 Kbps service for voice, voice/data, and, in GOSIP, OSI data. Both the basic and primary rates are needed. Later broadband ISDN (B-ISDN) is needed. The initial fundamental requirements are: 1) specifications enabling multi-vendor interconnection compatibility between terminal equipment and switching equipment and 2) specifications enabling multi-vendor interconnection compatibility between switching equipment.

Status

The North American ISDN Users Forum (NIU-FORUM), comprising a user's workshop (IUW) and an implementor's workshop (IIW), is addressing issues of multi-vendor terminal equipment-to-switch and switch-to-switch interoperation and ISDN application profiles. Some implementation agreements and application profiles are expected by the end of 1990.

Plan

The GOSIP FIPS will reference appropriate IIW agreements and ISDN FIPS as they become available. NIST plans to issue ISDN FIPS for integrated voice, image, data, and video and non-OSI data, as appropriate agreements are achieved in the IIW and IUW. The primary requirement for ISDN in GOSIP is as a network bearer service accessible via terminal equipment and switching equipment that can be connected readily, regardless of the specific vendor. The GOSIP FIPS will evolve to account for availability of B-ISDN and the Synchronized Optical Network (SONET).

APPENDIX 6. ACRONYMS

ACSE	Association Control Service Element
AE	Application Entity
AFI	Authority and Format Identifier
ANSI	American National Standards Institute
AP	Application Profile
ASCII	American Standard Code for Information Interchange
ASN	Abstract Syntax Notation
BRI	Basic Rate Interface
CCITT	Consultative Committee for International Telegraph & Telephone
CGM	Computer Graphics Metafile
CLNP	Connectionless Network Protocol
CLNS	Connectionless Network Service
CLTP	Connectionless Transport Protocol
CLTS	Connectionless Transport Service
CMIP	Common Management Information Protocol
CMIS	Common Management Information Services
CONS	Connection-Oriented Network Service
COTS	Connection-Oriented Transport Service
CSMA/CD	Carrier Sense, Multiple Access with Collision Detection
DAP	Document Application Profile
DIS	Draft International Standard
DOD	Department of Defense
DOE	Department of Energy
DP	Draft Proposal
DSP	Domain Specific Part
DTR	Draft Technical Report
ECMA	European Computer Manufacturers Association
EIA	Electronic Industries Association
ES-IS	End System-Intermediate System
FADU	File Access Data Unit
FAR	Federal Acquisition Regulation
FDDI	Fiber Distributed Data Interface
FIB	Forwarding Information Base
FIPS	Federal Information Processing Standard
FIRMR	Federal Information Resources Management Regulation
FTAM	File Transfer, Access, and Management
GENSER	General Service
GOSIP	Government Open Systems Interconnection Profile
GSA	General Services Administration
HDLC	High Level Data Link Control
ICD	International Code Designator
IDI	Initial Domain Identifier
IDP	Initial Domain Part
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IRV	International Reference Version
IS	International Standard
IS	Intermediate System
IS-IS	Intermediate System-Intermediate System
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization

JTC	Joint Technical Committee
LAN	Local Area Network
LAPB	Link Access Procedure B
LAPD	Link Access Procedure D
MAC	Medium Access Control
MAP	Manufacturing Automation Protocol
MHS	Message Handling Systems
MMS	Manufacturing Message Specification
NCS	National Communications System
NIST	National Institute of Standards and Technology
NMSIG	Network Management Special Interest Group
NPDU	Network Protocol Data Unit
NPAI	Network Protocol Access Information
NSA	National Security Agency
NSAP	Network Service Access Point
ODA	Office Document Architecture
OSIO	Open Systems Interconnection
PCI	Protocol Control Information
PDN	Public Data Network
PDU	Protocol Data Unit
PHY	Physical Layer Protocol
PLP	Packet Level Protocol
PMD	Physical Medium Dependent
PRI	Primary Rate Interface
PSAP	Presentation Service Access Point
RDA	Remote Database Access
RFP	Request For Proposal
RIB	Routing Information Base
SAP	Service Access Point
SC	Steering Committee
SCI	Special Compartmented Information
SDNS	Secure Data Network Service
SGML	Standard Generalized Markup Language
SIG	Special Interest Group
SILS	Standard for Interoperable LAN Security
SIOP-ESI	Single Integrated Operational Plan-Extremely Sensitive Info.
SMT	Station Management
SNPA	Subnetwork Point of Attachment
SQL	Structured Query Language
SSAP	Session Service Access Point
SVC	Switched Virtual Circuit
TC	Technical Committee
TOP	Technical and Office Protocols
TP	Transaction Processing
TSAP	Transport Service Access Point
TTY	Teletype
VT	Virtual Terminal
WAN	Wide Area Network
WG	Working Group
WYSIWYG	What You See Is What You Get