NASA Contractor Report 177561

OSI in the NASA Science Internet – An Analysis

Rebecca Nitzan

CONTRACT NAS2-11555
June 1990

National Aeronautics and
Space Administration

NASA Contractor Report 177561

OSI in the NASA Science Internet – An Analysis

Rebecca Nitzan

Sterling Federal Systems, Inc.
Palo Alto, California

Prepared for
Ames Research Center
CONTRACT NAS2-11555
June 1990

National Aeronautics and
Space Administration

Ames Research Center
Moffett Field, California 94035-1000

Contents

Acknowledgments v

1.0 Summary 1

2.0 Introduction 4
2.1 Scope 4
2.2 Objectives 4
2.3 Information Dissemination and Review . . 5
2.4 Format of Paper 5

3.0 NSI Components 6
3.1 The Space Physics Analysis Network . . 6
3.2 The NASA Science Network 6

4.0 Overview of OSI 9
4.1 Concerns Regarding OSI 9
4.2 OSI Reference Model 10
4.3 Lower-Layer End-to-End Service . . . 11
4.4 Upper-Layer User Application Services . . 12
4.4.1 File Transfer, Access and Management . 13
4.4.2 Message Handling System (X.400) . . 14
4.4.3 Virtual Terminal 14
4.4.4 ISO Development Environment . . 14
4.5 Status of OSI Development 14
4.6 Address and Name Registration . . . 15
4.7 The Government OSI Profile 18

5.0 Considerations for OSI Integration 19

6.0 OSI and NSI 22
6.1 OSI and NSN 22
6.1.1 Staged Integration: First Stage - Fiscal Year 1991 22
6.2 OSI and SPAN 23
6.2.1 Issues of the Existing DECnet Internet . 23
6.2.2 Phase V - Phase IV Interoperability . . 24
6.2.3 Naming and Directory Service Issues . 24
6.2.4 DNANS Interoperating with X.500 . . 25
6.2.5 Phase V Routing and Addressing . . 25

7.0 Possible Paths for OSI Integration in NSI . . . 26
7.1 Resultant NSI Structure and Goals . . . 26
7.2 NSI/OSI Addressing 27
7.3 NSI/OSI Routing 27
7.4 NSI/OSI Naming 27
7.5 NSI/OSI Network Management 27
7.6 Option 1: SPAN and NSN Integrate OSI Separately . 28
7.7 Option 2: SPAN and NSN Jointly Integrate OSI Including DECnet Phase V 31

Appendices

Appendix A:	OSI Standardization Procedures	34
Appendix B:	Network Service Access Point Structure	36
Appendix C:	U.S. GOSIP	38
Appendix D:	Routing Domains	41
Appendix E:	SPAN Phase V Transition Costs	44
Appendix F:	Nomenclature	48

References 50

Tables 52

Figures 52

Acknowledgments

A special thanks to Ms. Linda Porter (Marshall Space Flight Center) for her tireless help reviewing and contributing, especially in the SPAN network sections. Much appreciation is extended to Mr. John Cavallini (Department of Energy), Dr. Vint Cerf (Corporation for National Research Initiatives), Mr. Kevin Mills (National Institute of Standards and Technology), Dr. Marshall Rose (Performance Systems International), Mr. Peter Shames (Space Telescope Science Institute), and Mr. Warren Van Camp (Sterling Software) for their help reviewing this document. In addition, a thanks to the Federal Networking Council (FNC) OSI Planning Group (FOPG) for their help with the routing domain section.

1.0 SUMMARY

The Open Systems Interconnection (OSI) protocol suite is a result of a world-wide effort to develop international standards for networking. OSI is formalized through the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The goal of OSI is to provide interoperability between network products without relying on one particular vendor, and to do so on a multinational basis.

The National Institute for Standards and Technology (NIST) has developed a Government OSI Profile (GOSIP) (ref. 1) that specifies a subset of the OSI protocols as a Federal Information Processing Standard (FIPS 146). GOSIP compatibility has been adopted as the direction for all U.S. government networks. OSI is extremely diverse, and therefore adherence to a profile will facilitate interoperability within OSI networks. All major computer vendors have indicated current or future support of GOSIP-compliant OSI protocols in their products.

The NASA Science Internet (NSI) is an operational network, serving user requirements under NASA's Office of Space Science and Applications. NSI consists of the Space Physics Analysis Network (SPAN) that uses the DECnet* protocols and the NASA Science Network (NSN) that uses TCP/IP protocols (refs. 2, 3). The NSI Project Office is currently working on an OSI integration analysis and strategy. A long-term goal is to integrate SPAN and NSN into one unified network service, using a full OSI protocol suite, which will support the OSSA user community.

The switch to a new common networking technology is an enormous endeavor for existing network administrators and vendors alike. There are many problems to resolve and items to consider. Despite the issues, the momentum behind OSI is large, and OSI is anticipated to be in widespread use within the next five to eight years.

In order to realistically understand the situation, there are several items to consider:

- o A complete OSI protocol suite is still under development
- o Vendor products currently are not widely available
- o OSI is very diverse, with many protocols and options that may be used
- o Adherence to an OSI profile (such as GOSIP) is necessary for interoperability within an OSI network

OSI has been under development for 12 years. A complete OSI protocol suite is not anticipated to be in place until 1995 at the earliest. Interim solutions for key missing OSI protocols must be supplied in order to use OSI network services. Vital OSI protocols that are necessary for an operational network and that are still under development are shown in table 1 below.

** DECnet is a trademark of Digital Equipment Corporation.*

Table 1. OSI Protocols Required for an Operational Network

OSI Feature	Current International Standard Status	Time Estimate for Product Availability
Directory Service, X.500	Draft International Standard	1992
Dynamic Intradomain Routing	Draft Proposal	1991
Dynamic Interdomain Routing	Working Draft	1995
Network Management	Draft Proposal and Standard	1995

It is important that the integration of OSI products have minimal disruption on existing network operations and functionality. It is important that users do not suffer degradation of network services. OSI integration will be done as it becomes technically feasible. This involves coexistence and interoperability between OSI and the other widely used protocols within the NSI, DECnet, and TCP/IP. DEC is providing interoperability with DECnet Phase IV and DEC's next-generation networking architecture (Phase V) which is a partial OSI protocol stack.

NSI plans to:

- o Update OSI planning documents as integration evolves.
- o Develop a testbed implementation for OSI application services (e.g., file transfer and electronic mail).
- o Upgrade SPAN to DECnet Phase V (expected to start in 1990-1991).
- o Upgrade backbone routers to support ISO 8473 forwarding and dynamic intradomain routing (expected to start in 1990-1991).
- o Plan procedures for management and operations of the OSI backbone.
- o Develop NSI procedures for address/name registration and dissemination, in coordination with other NASA OSI network administrators.
- o Engineer routing domain and area boundaries for NSI, in coordination with NASA and other agency OSI network administrators.

No precise blueprint for full stack OSI integration can be drafted until OSI protocols are more fully developed, commercial offerings are on the market, and user needs are

clearer. However, NSI is taking steps to prepare a solid foundation for the future integration of OSI protocols.

Support of a full OSI protocol suite will be a long-term endeavor for the NSI Project Office as well as for the NSI user community. There are still many issues that need to be solved before an operational network, based completely on OSI protocol standards, is in place. During this integration period, existing services based on the DECnet and TCP/IP protocols will need to coexist with OSI, and in some cases interoperate.

2.0 INTRODUCTION

There is a major multinational thrust to move networking technology towards one common set of protocols, the Open Systems Interconnection (OSI). The intent is for all networks to move away from using diverse protocols and gain interoperability by using one common protocol suite. Given the premise that there will most assuredly be an eventual widespread integration of OSI within the next three to five years, the National Aeronautics and Space Administration (NASA) is now planning for OSI. This document analyzes the issues and steps involved in integrating OSI into the NASA Science Internet (NSI).

It is recognized that there is a commitment to integrate OSI into a government agency such as NASA. However, it must also be recognized that there is a higher commitment to continue providing existing network services to users. Therefore, in addition to the integration of OSI, coexistence and interoperability must be achieved among OSI and other widely used protocols within NASA.

The integration and use of any new protocols in a large established network may require adjustments or fine tuning to the protocols themselves as well as to how they are used. This is a normal expectation for changes of this magnitude which will affect thousands of NASA host computers. This paper identifies some of the issues and potential problems that may arise as the new OSI protocols are integrated. This is an important part of the initial planning stage.

2.1 Scope

The scope of this document includes the integration of OSI into NSI's existing operational science networks which use the Digital Equipment Corporation networking protocols (DECnet) Phase IV and the Department of Defense (DOD) Internet Protocols (ref. 2) commonly referred to as TCP/IP. (TCP stands for the Transmission Control Protocol, ref. 3.) Any other protocols are beyond the scope of this document. It is also necessary to consider how OSI plans will affect other NASA networks as well as other agency networks which interconnect to NSI networks, such as NASA's Numeric Aerodynamic Simulator Network (NASNET) or the National Science Foundation Network (NSFNET). In addition, the implications of OSI and the Government OSI Profile (GOSIP) (ref. 1) are considered.

2.2 Objectives

The goals of this document are (1) to provide a two- to three-year analysis for a strategic plan for integrating OSI into NSI, and (2) to provide technical information about OSI. The plan will in fact evolve and will be updated in an ongoing effort because the OSI protocols are still under development (i.e., there will not be a complete protocol suite until at least 1995), and because commercial OSI products are not widely available. This document is largely informational at this time.

Given the constraints above, the objective is to identify issues, tasks, schedules, costs, and resources needed to integrate OSI into the NASA Science Internet.

2.3 Information Dissemination and Review

It is important that information on OSI planning reach all of those in the NSI community who are involved and will be potentially affected, e.g., user sites and center network managers. Feedback from the user community is extremely important to NSI and is encouraged. This collaboration is necessary for several reasons: (1) the OSI technology will bring together networks that have in the past been disjoint due to the usage of different networking protocols, and (2) the user community should be involved in planning which may affect them.

This document will be reviewed by the NSI Project Office (NSIPO), the Space Physics Analysis Network (SPAN) management, and the NASA Science Network (NSN) management. In addition, this document will be made available for comment by other agencies that interconnect to NSI and that intend to integrate OSI as well. These reviews are considered an important effort to minimize disruption and maintain interoperability with the future OSI networks. All feedback is encouraged and highly valued.

2.4 Format of Paper

After a brief summary of NSI, there is an overview of OSI, followed by detailed considerations of OSI issues. Then several strategic approaches for NSI's integration of OSI are discussed.

3.0 NSI COMPONENTS

NSI was developed to support NASA's Office of Space Science and Applications (OSSA) research programs and flight missions, including joint research projects between NASA, other agencies, and international organizations. NSI is an open network providing engineering, operations support, and user services to a broad community of users throughout NASA and other research centers world-wide. The NSI users, in addition to communicating with each other via the NSI networks, communicate with users and resources on other networks thus reaching many tens of thousands of scientists and science data systems all over the world.

There are two NSI networks, SPAN and NSN (see figs. 1 and 2).

3.1 The Space Physics Analysis Network

The SPAN network connects more than 100 research sites in the United States, Europe, Canada, and Japan. NASA scientists at these sites use the Digital Equipment Corporation Network protocols (DECnet). SPAN also connects to several other large DECnet networks such as the DECnet portion of the Energy Science Network (ESNET/DECnet), the European SPAN, and the European High Energy Physics Network. This connectivity creates one of the largest DECnet Internets in the world, in excess of 20,000 nodes.

SPAN also connects to NSN at all NASA centers where both networks coexist. There are several mail gateways, and one file transfer and virtual terminal gateway providing interoperability between SPAN and NSN.

SPAN provides distributed network support services through SPAN "routing centers" which are located at each of the major NASA centers. The SPAN project office is located at the Goddard Space Flight Center (GSFC) in Maryland.

3.2 The NASA Science Network

The NASA Science Network (NSN) provides network services using the Transport Control Protocol (TCP) and the Internet Protocol (IP). The TCP/IP protocol suite is nonproprietary with many researchers, vendors, and users contributing to its ongoing standards development. The NSN also has interagency connections to other major networks, such as the National Science Foundation Network (NSFNET), the Energy Science Network (ESNET), regional networks, and the MILNET portion of the Defense Data Network (DDN). These networks, which are IP based, also interconnect to the world-wide Internet which includes approximately 2,000 networks and 200,000 hosts used by more than 1 million users.

The NSN is centrally operated and managed at the Ames Research Center (ARC) in California. NSN provides 24-hour-a-day, 7-day-a-week network operations service.

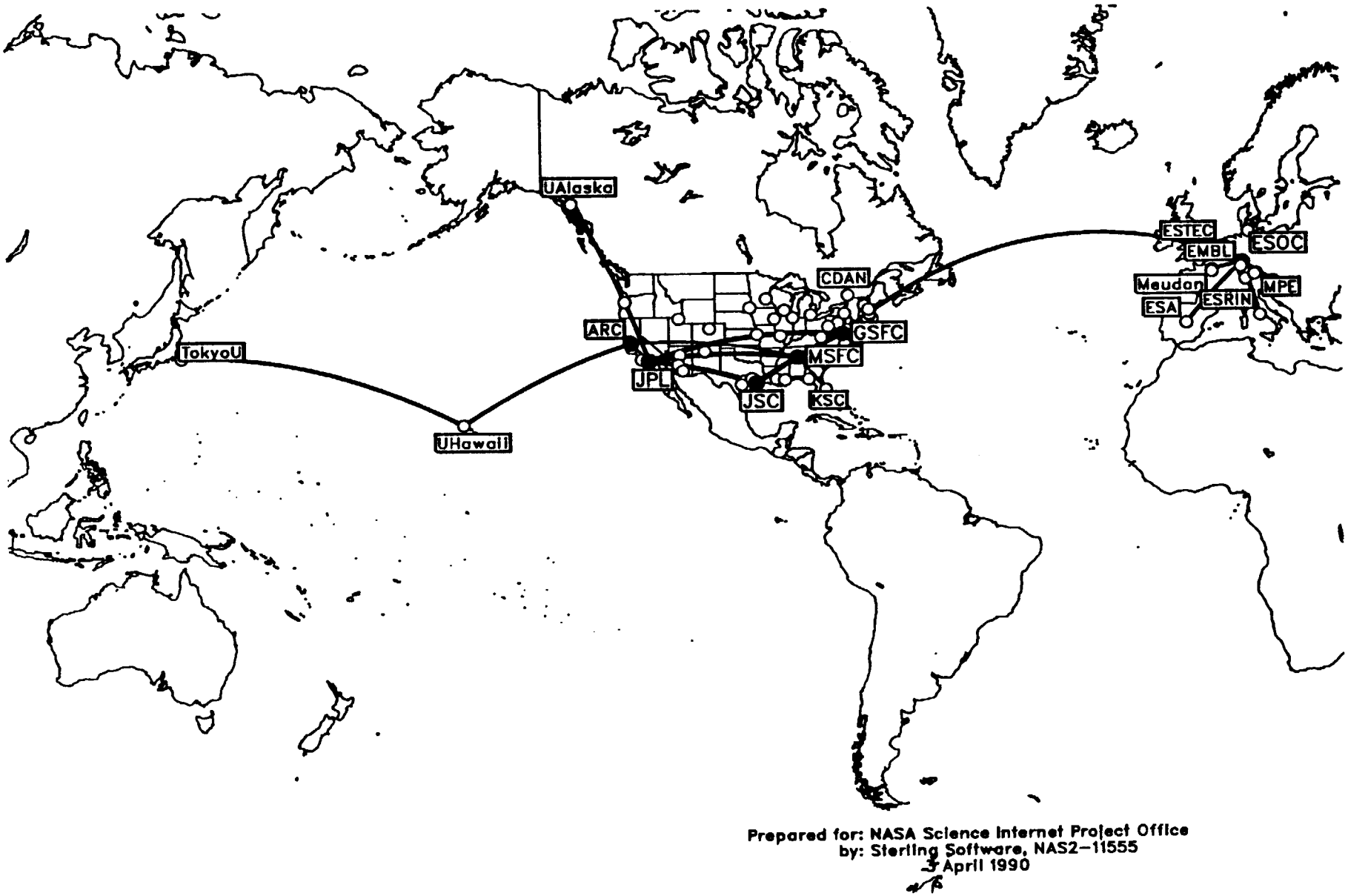


Figure 1.- Space Physics Analysis Network (SPAN).

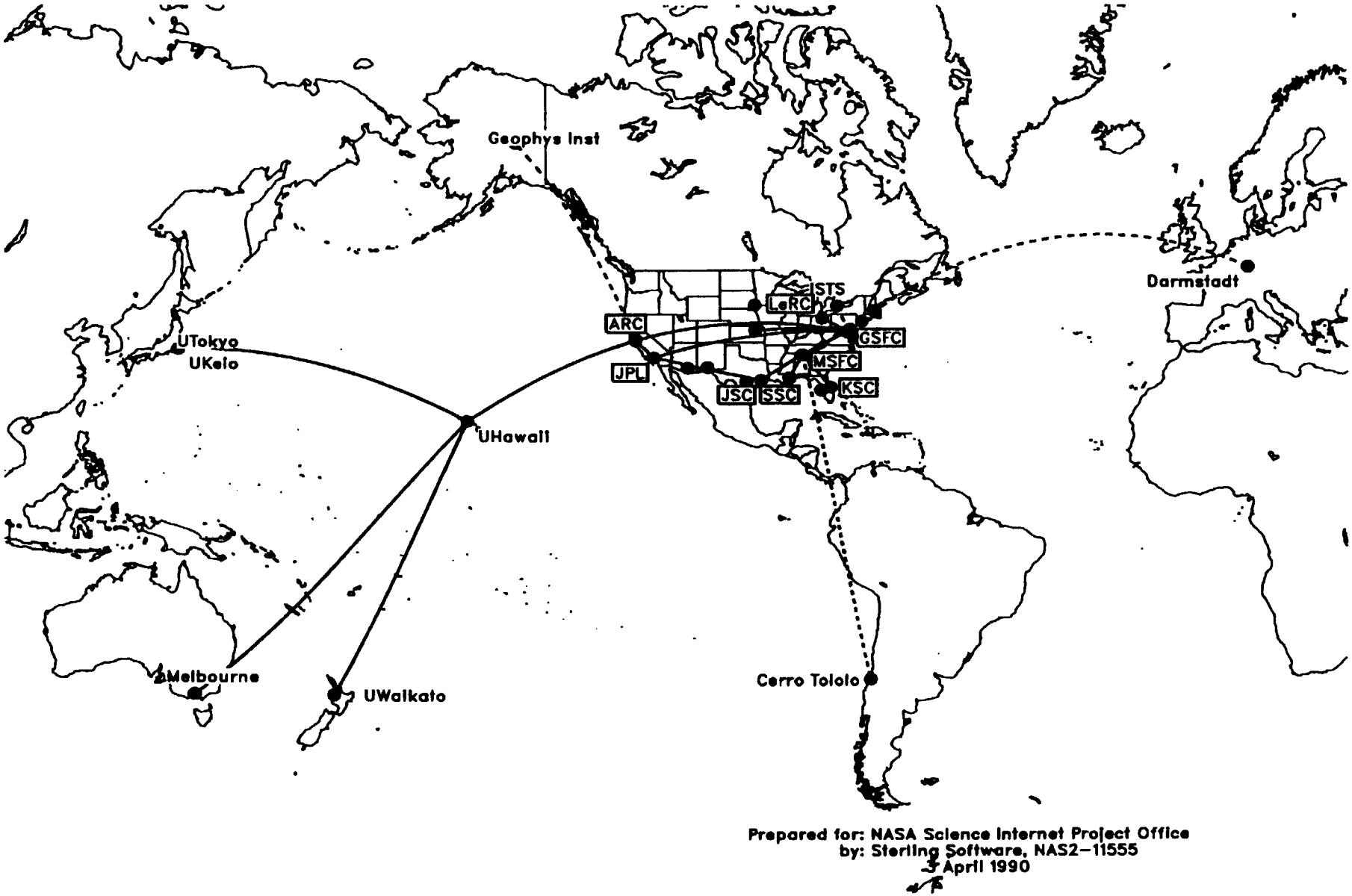


Figure 2.- NASA Science Network (NSN).

4.0 OVERVIEW OF OSI

The development of OSI networking technology is a world-wide international effort. Many countries participate in the effort to develop OSI technology through various committees such as the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the International Telegraph and Telephone Consultative Committee (CCITT).

The United States is represented by the American National Standards Institute (ANSI). ANSI members represent commercial vendors as well as government agencies such as NASA and the Systems and Network Architecture Division of the National Institute of Standards and Technology (NIST).

The goal of OSI is to agree on one international standard for networking protocols to achieve the following results:

- o Enhanced interoperability
- o Enhanced user application services
- o A more competitive vendor market in networking products
- o A forum to standardize new networking technology
- o Cost savings

4.1 Concerns Regarding OSI

While the anticipated benefits of OSI are clearly desirable, there is concern that attaining these results will be difficult due to technical and management issues.

In order to achieve interoperability within the OSI protocol suite itself, there must be coordinated choices made between networks that wish to interoperate. One difficulty with OSI is that it has many diverse options and refinements to options, many of which are incompatible. As a result, further definitions and guidelines on how to specifically apply the OSI protocols are required. These guidelines are referred to as "profiles." The U.S. government has developed the Government OSI Profile (GOSIP) (ref. 1), and other countries are developing their own profiles as well. One problem is that some of these OSI profiles are not compatible with each other, such as the U.S. GOSIP and the U.K. GOSIP. The lack of alignment between profiles is largely due to national network preferences. Unfortunately, the result will be a lack of interoperability.

There has also been concern among the networking community about the sluggishness of the standards organizations in developing the necessary technology. The minimum time it takes a proposed standard to become a full International Standard is two years. The OSI protocol suite has been a 12-year project so far, and it still lacks some protocols needed to support a solid infrastructure. (See App. A, OSI Standardization Procedures.)

Despite these difficulties, there is a large momentum behind the OSI development, and it is anticipated to be in wide use eventually. Some of the most optimistic speculation has been that OSI will be in wide use five years from now, while the more pessimistic speculation is that it will take another ten years.

Regardless of speculation, full integration of OSI is not possible today. Therefore, we must achieve coexistence and interoperability between OSI and the operationally used protocols in NSI (DECnet and TCP/IP).

Full integration, in the case of an existing network, means actually converting the network software, and potentially the hardware, from one protocol suite to another. It is clear that interoperability and coexistence between OSI and other protocols will provide the most workable interim solution for users during the integration period.

Coexistence among protocol suites occurs when separate protocols run in parallel on the same network. This can be accomplished by multiple protocol stacks (e.g., TCP/IP and DECnet Phase IV), by encapsulation, or by operating physically separate networks.

Communication between two machines is accomplished by a common set of network protocols, which allows different vendor products to communicate, provided the same standard protocols are used. This becomes quite complicated when one machine uses a different protocol suite than the other machine. Some type of conversion mechanism is required between the two protocols. This is typically accomplished by "application gateways" for a limited set of applications such as file transfer, electronic mail, and remote terminal access.

4.2 OSI Reference Model

The OSI reference model (ref. 4) is divided into seven layers, where the lower layers are closer to the physical medium and the upper layers are closer to the user applications (fig. 3). Typically, each of the OSI protocols can be categorized into layers. This reference model has been a very useful mechanism for describing other protocol suites as well.

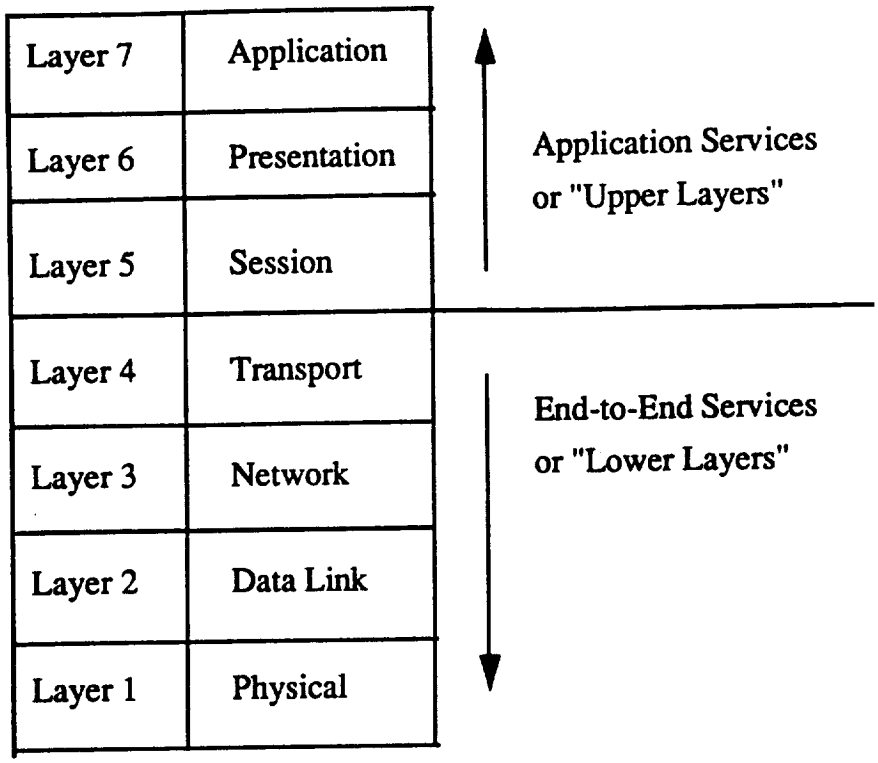


Figure 3. - The Seven-Layer OSI Reference Model.

The upper three layers comprise the application services, such as electronic mail or file transfer. The lower four layers comprise the end-to-end services.

4.3 Lower-Layer End-to-End Service

The transport, network, data link, and physical layer protocols combine to provide an "end-to-end" network service which is responsible for actually getting the data from one machine to another intact. The end-to-end service is defined in terms of the protocols running in the "lower layers" (fig. 4).

Layer 4	Transport
Layer 3	Network
Layer 2	Data Link
Layer 1	Physical

Figure 4. - The Lower Layers of the OSI Reference Model.

OSI recognizes two types of network service, the Connection-Oriented Network Service (CONS) and the Connectionless Network Service (CLNS). CONS is used throughout Europe in conjunction with the X.25 protocol. The U.S. research community mainly uses CLNS which is similar in concept to the network service provided by the Internet Protocol (IP). CLNS is implemented with the protocol described in ISO 8473 (ref. 5). The ISO 8473 protocol is also commonly referred to as the Connectionless Network-layer Protocol (CLNP) and as ISO IP, however, throughout this document it is referred to as ISO 8473.

There are questions regarding the interoperability of CONS and CLNS which raise the issue of how to interoperate efficiently between a CONS network and a CLNS network. There are pros and cons to both CLNS and CONS, yet the optimal solution is for the entire world to use one type of network service. Unfortunately, this type of international agreement has not been possible.

OSI has five transport services. The first four of them, TP0-TP3, assume a reliable underlying virtual circuit (e.g., X.25). The other transport protocol, TP4, is a reliable transport service similar to TCP. TP4 does not assume a reliable virtual circuit and may be run over ISO 8473.

End-to-end network service between two computers is optimal when they use the same transport and network protocols. If these protocols are different, then an additional mechanism to facilitate communication will be required. Since there are two end-to-end network services that will be used widely, CONS and CLNS, there may be a need for such a mechanism.

4.4 Upper-Layer User Application Services

A compelling reason for using OSI protocols will be enhanced user application services, e.g., multimedia Message Handling Systems. OSI will eventually offer improved application services as well as multivendor product availability.

The application service can be thought of in terms of the "upper layers"; application, presentation, and session (fig. 5).

Layer 7	Application
Layer 6	Presentation
Layer 5	Session

Figure 5. - The Upper Layers of the OSI Reference Model.

The protocols in these layers comprise the application services.

There are two ways an end system user can make use of OSI application services: (1) Have lower-layer OSI end-to-end service support so that the upper-layer applications can traverse a network to get to the destination. This may be accomplished on a small scale; however, on a large scale, the lack of a complete OSI protocol suite will cause suboptimal results compared to the existing network technologies. (2) Use OSI application software that runs on top of an end-to-end service that is currently supported (e.g., TCP/IP). Software that is currently available to do this is the ISO Development Environment (ISODE) which is capable of running OSI application services on TCP/IP lower layers (ref. 6). See section 4.4.4. for additional information on ISODE.

The most common user-application services utilized on a network are file transfer, electronic mail, and remote terminal access. The following three sections briefly explain the OSI version of these application services.

4.4.1 File Transfer, Access, and Management

The File Transfer, Access, and Management (FTAM) (ref. 7) provides file management. The simpler aspects of FTAM, such as file transfer, are similar to the TCP/IP File Transfer Protocol (FTP) (ref. 8) and are somewhat similar to DECnet "COPY."

The FTAM file service also provides other more complex capabilities, such as accessing structured portions of a file, remote database access, and diskless workstation access.

File manipulation on a system is very much operating-system dependent. Therefore, FTAM is defined in terms of a "virtual filestore," which is designed to be independent of the operating system (there must be a specific interface provided between FTAM and the particular operating system). FTAM has the advantage of being very general, however, this could result in a file service that has less functionality and performance than a file service that is customized and fine tuned for a particular operating system.

4.4.2 Message Handling System (X.400)

The Message Handling System (MHS) supports one of the most popular applications on a network, electronic mail. It is based on the CCITT Recommendation X.400 (ref. 9). X.400's electronic mail facility is similar, but richer in functionality, to the TCP/IP Simple Mail Transfer Protocol (SMTP) (ref. 10). The X.400 MHS will eventually have features which can support multimedia messaging including facsimile, voice, and teletex, in addition to ASCII text. There still is much work to be done before X.400 will offer users this additional functionality.

4.4.3 Virtual Terminal

The Virtual Terminal Protocol (VTP) (ref. 11) provides remote terminal access capabilities to users who want to connect to a target computer via another computer. The VTP TELNET profile is similar to the TELNET (ref. 12) protocol used in the Internet, or DECnet "SET HOST." The VTP forms profile is similar to terminals which have an intelligent editing and display capability.

4.4.4 ISO Development Environment

The ISO Development Environment (ISODE) provides public domain software supporting some OSI applications over a TCP/IP end-to-end network service. Since some of the OSI lower layers are an issue, running OSI applications over TCP/IP is a workable interim solution for some cases.

ISODE was originally developed as a test-bed implementation of OSI upper-layer services. Marshall Rose is largely responsible for this effort. The ISODE software will become available in several vendor products. The applications provided include File Transfer, Access, and Management (FTAM), and OSI Virtual Terminal Protocol (VTP), among others. For more information on ISODE see Marshall Rose's *The Open Book* (ref. 13).

4.5 Status of OSI Development

The OSI infrastructure still lacks a few vital pieces for a complete OSI operational network. Until these items are available on the market as OSI International Standards, alternative means to provide the needed functionality (see the schedule shown table 2 of OSI standards) will be needed. Some interim solutions may be vendor specific (e.g., DECnet Phase V uses some DECnet protocols), and some will be other standards, such as those being developed under the TCP/IP protocol suite. Vendor-specific solutions will probably not interoperate with other vendor solutions or with interim standards.

Table 2. Product Availability for Key OSI Features

OSI Feature	Current International Standard Status	Time Estimate for Product Availability
Directory Service X.500	Draft International Standard	1992
Dynamic Intradomain Routing	Draft Proposal	1991
Dynamic Interdomain Routing	Working Draft	1995
Network Management	Draft Proposal and Standard	1995

Table 2 provides an estimate of product availability for the OSI key missing pieces. At present, interdomain routing is done with static routing tables. (See App. A, OSI Standardization Procedures, for descriptions of the standards status.)

4.6 Address and Name Registration

All end systems (also known as hosts or nodes) and intermediate systems (IS, also known as routers or gateways), need a unique way in which to be identified in order to communicate. This is accomplished by using a unique name and number identification. Since the systems within NASA networks communicate with other networks throughout the world, a registration procedure must be followed to ensure that the identification is unique world-wide.

The Systems and Network Architecture Division at NIST determines how government agency-specific identifications are assigned and registered at the national level. NIST has delegated this task to the Telecommunications Customer Service Division within the General Services Administration (GSA). At this time the GSA is still defining the registration procedures as well as usage guidelines.

Systems are identified by unique names and numeric addresses, similar to how people are identifiable by their names and social security numbers. Both names and addresses are hierarchically defined. The hierarchy is used both for registration purposes as well as for routing purposes. For example, upper portions of the NSAP address are registered and disseminated by international organizations. Then the lower portions of an NSAP address are further registered and disseminated by a particular organization within a country. Routing is based on the hierarchical structure of the NSAP address as well. However, further discussion of this is beyond the scope of this document. The hierarchical tree structure in figure 6 shows the upper portion of a name or address. A subportion of the hierarchical tree may be delegated to an agency or network administrator, along with the responsibility of further disseminating the addresses or names. The unique identifications are referred to as object identifiers.

There are two advantages for having a hierarchy: (1) the scheme provides a world-wide addressing mechanism, and (2) it enables routing table information collapse.

These advantages will become more and more apparent as the network user base continues to grow in size.

The hierarchical scheme does cause additional consideration for the following reason: the way the identifications are administratively assigned and disseminated does not necessarily fit into how the routing should be engineered. For example, in order to reduce the amount of routing information in a router, it may be necessary to assign Administrative Authority identifications to networks that do not necessarily affiliate themselves with the U.S. government. In addition, a network may be so small that it could never possibly make use of all the address space provided below the Administrative Authority field. (For additional clarification, see Appendices B and D, NSAP Address Structure, and Routing Domains.)

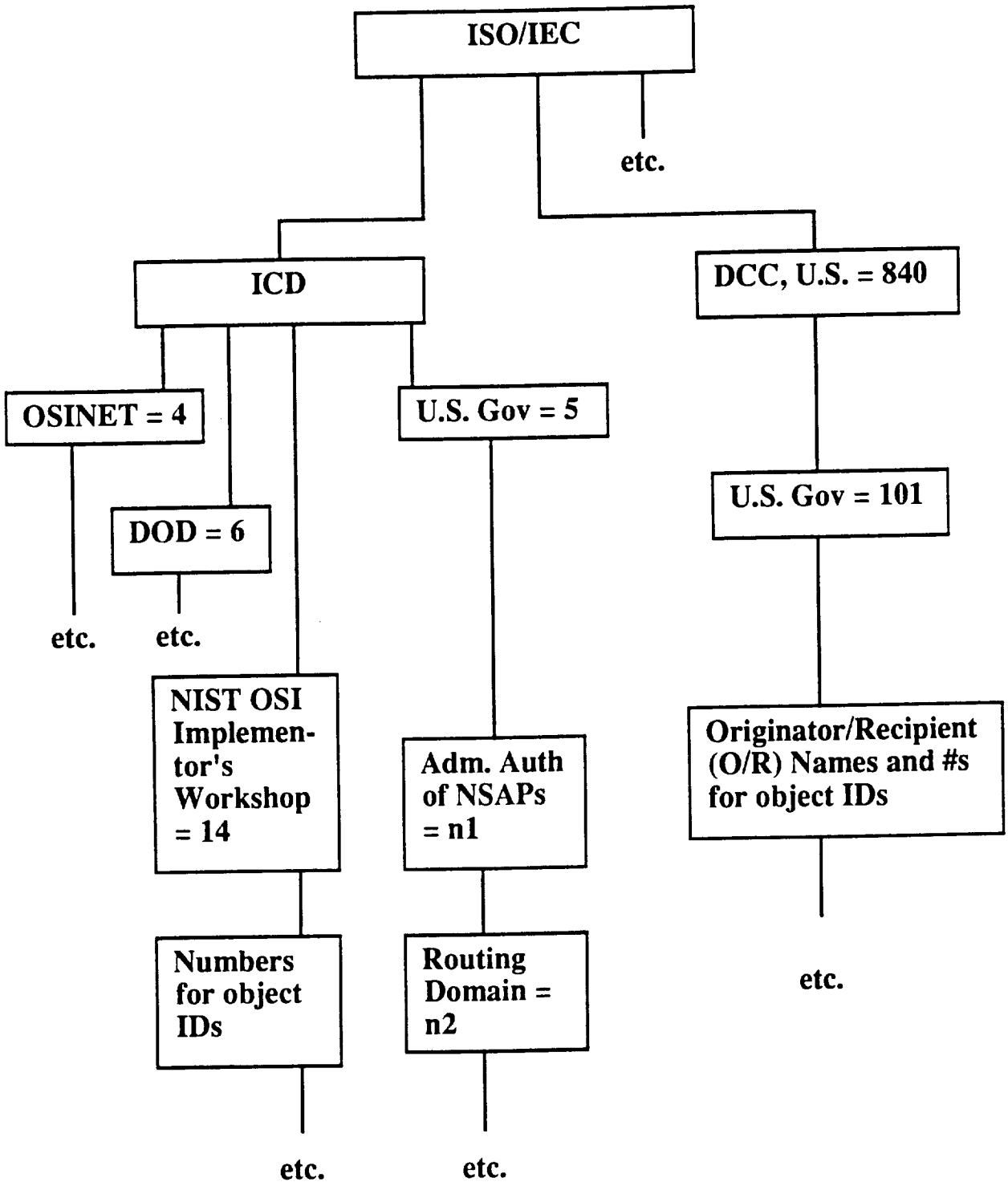


Figure 6.- Currently Defined Portions of a Complete NSAP Address or Name

The partial tree-like structure in figure 6 illustrates currently defined portions of a complete NSAP address or name, such as the International Code Designator (ICD) = 4, and the Data Country Code (DCC) = 840. The ISO/IEC assigned the ICD to NIST and the DCC to ANSI. NIST then gave OSINET and the U.S. government the Initial Domain Identifiers (IDI) 4 and 5, respectively. NIST applied on behalf of DOD to obtain an ICD, 6, which is now owned by DOD (see App. B, Network Service Access Point Structure). NIST also applied on behalf of the OSI Implementors' Workshop for ICD, 14, which assigns technical objects such as FTAM document type and VT profiles. This diagram is only partially complete; there are many other items that have been disseminated. The Network Service Access Point (NSAP) is the numeric identification of an OSI end system.

Within the NSIPO there will be a centralized process for address and name registration.

The Originator/Recipient (O/R) name and portions of the NSAP numbers will be registered and handed out by the General Services Administration (GSA), along with guidelines on usage (see App. B for details on the NSAP address format). NIST has delegated this authority to the GSA. The GSA intends to define whether the O/R name is used as a Private Management Domain (PRMD), or an Administrative Management Domain (ADMD) or an Organizational Unit, etc. Currently the details of this procedure are unresolved.

4.7 The Government OSI Profile

The Federal Information Processing Standard (FIPS) 146 Publication on the Government OSI Profile (GOSIP) (ref.1) specifies OSI protocols, options, and refinements to use in Government OSI networks. OSI has many options to use; therefore, a profile such as GOSIP is necessary to facilitate interoperability within government OSI networks.

However, citing GOSIP is not a requirement when OSI does not provide a feasible solution for existing operational non-OSI networks. OSI is still under development, and vendor products are not widely available. Therefore, it is anticipated that GOSIP will not be feasible in many near-term cases and will not be applicable during the procurement process. [For additional information on GOSIP, see the GOSIP Users' Guide (ref. 14), and App. C, U.S. GOSIP.]

5.0 CONSIDERATIONS FOR OSI INTEGRATION

In developing strategic plans for the short- to mid-term time-frame (i.e., two to three years), one must consider factors which may impact or drive these plans. A complete OSI protocol suite is still under development, which impacts designing specific implementation plans. The expected date for completion of OSI standards is a moving target. In addition, the plans may change as more is learned about the capabilities and details of the OSI Protocols. Networking technology is moving forward rapidly in OSI as well as in other networking standards. Therefore, planning will continue to evolve and change where necessary to take advantage of trends in the field.

The plan for an OSI environment will most certainly be tempered by the following requirements:

- o Minimal Disruption to Operational Networks
- o Coexistence with Other Protocols
- o GOSIP Compliance
- o Integration of OSI into TCP/IP Networks
- o Integration of OSI into DECnet Phase IV Networks
- o Interoperability Between Protocols

(1) Minimal Disruption to Operational Networks

Probably one of the most important requirements is to have minimal disruption to existing network services to users during the OSI integration period. While it is recognized that some level of disruption is unavoidable, that level should be kept to a minimum, similar to any system software upgrade. An alternate fall-back plan should be in place for those facing any extended unplanned disruption. Specifically, disruption must be avoided during flight projects.

(2) Coexistence with Other Protocols

In order to effect a smooth integration of OSI, there will be a definite time frame where OSI and other protocols, such as TCP/IP and DECnet Phase IV, will be required for some extended time. In fact, some speculate that TCP/IP will still be in widespread use for the next five to ten years. It will be necessary to ensure that OSI coexists with TCP/IP and DECnet Phase IV, since a nondisrupted operational network is a requirement.

(3) GOSIP Compliance

The U.S. GOSIP is important because it will facilitate procuring interoperable products for U.S. government OSI networks. It is important because OSI is diverse with many potential options. A profile indicating a subset of OSI, as well as refinements to options within OSI, can be cited when procuring OSI network products. In some cases, especially where the network is an existing non-OSI network, GOSIP may not be required for certain procurement specifications. GOSIP may be applicable when procuring new network services or major network service upgrade. However, the applicability of GOSIP in these cases will depend on whether products are available and whether they will interoperate with the existing network to meet requirements.

Clearly, when specific OSI products are acquired, they must meet the GOSIP specifications.

(4) Integration of OSI into TCP/IP Networks

As the OSI protocols become mature, existing TCP/IP networks will start phasing them in. For example, NSFNET is running ISO 8473 in a test-bed environment with operational service most likely to start in 1990 or early 1991. Other networks such as NSN, ESNET, and regional networks are also planning to provide ISO 8473 service shortly. Most router vendors already offer this software capability.

It is estimated that this integration will be gradual with momentum picking up as the OSI protocols become increasingly widespread. OSI usage will naturally increase as the advantages become apparent.

(5) Upgrade to DECnet Phase V

NSI's current DECnet Phase IV network, SPAN, faces the issue of upgrading to DECnet Phase V, which includes some OSI as well. The primary reason for this upgrade is the address limitations in the current DECnet Phase IV network. Each node in the network needs an address; therefore, the result of this address limitation is that the growth of the network is limited by not enough network address numbers (see section 6.2.1, Issues of the Existing DECnet Internet). Phase V uses the OSI NSAP address structure, which has a huge amount of address space. Therefore, after Phase V is fully integrated, it will solve the address limitation problem of DECnet Phase IV. It will also include some of the OSI standards, e.g., those which are indicated in GOSIP. Note that Phase V provides its own DEC solutions for the portions of the OSI technology which are not yet fully developed and standardized which are necessary for an operational network (i.e., directory services, interdomain routing, and network management).

(6) Interoperability Between Protocols

Interoperability between the following protocols is required by NSI:

- o DECnet Phase IV and TCP/IP
- o DECnet Phase IV and DECnet Phase V
- o DECnet Phase V and TCP/IP
- o TCP/IP and OSI
- o DECnet Phase V and OSI (possibly)

Interoperability between DECnet Phase IV and DECnet Phase V is provided with DEC Phase V routers. Gateway products currently exist to provide basic interoperability between DECnet Phase IV and TCP/IP.

Achieving interoperability between computers using different protocols can be a complex problem, one in which efficient solutions can take significant time and effort to develop. In most situations, some compromise in performance

and functionality is a result. This is an area for further research, even though there have been several solutions developed already. For example, the application gateways and transport service bridges (ref. 13).

(7) Interoperability Within OSI

Since there are many types of end-to-end and application services in OSI from which to choose, there is an interoperability issue within the OSI technology itself. For example, CLNS and CONS are incompatible. The issue of CLNS vs CONS will become increasingly significant, especially as NASA and the United States in general continue to expand connectivity into European sites, since Europe tends to use CONS and the United States tends to use CLNS. It should also be noted that the use of CLNS in Europe is growing.

6.0 OSI AND NSI

Both NSN and SPAN are working with other government agencies on the OSI issues. This is considered important, since coordination will result in interoperability between the U.S. government networks, research laboratories, and universities. In particular, a focus is on gearing decisions towards optimal long-term solutions as well as short-term solutions that will work and interoperate.

The agencies involved with this collaboration, in addition to NASA's NSI, are DOE and NSF, with representatives of both TCP/IP and DECnet communities.

6.1 OSI and NSN

There is a large TCP/IP user community relying on the uninterrupted service provided by NSN and the Internet. Therefore, a multiprotocol network will be needed for quite some time. For the next five years, coexistence as well as interoperability between OSI and TCP/IP will also be required.

The type of interoperability needed largely depends on NASA's user application requirements. Typically the main uses across a network are electronic mail, file transfer, and remote terminal access, and there are other project specific requirements as well.

Since the OSI protocol suite is not complete, integrating new OSI services must be done carefully. It is important to acquire OSI products that will interoperate and that will not result in a reliance on vendor-specific solutions for the incomplete OSI protocols. OSI protocols will be integrated gradually as they become commercially available and as they provide equivalent or enhanced capabilities compared to what is currently available.

6.1.1 Staged Integration: First Stage - Fiscal Year 1991

The timeframe for OSI integration is anticipated to be a several-year period with various degrees of OSI usage at each stage.

During the first stage of integration there are two items to consider; (1) the end systems (hosts), and (2) the intermediate systems (backbone routers). These two items go hand in hand. User needs must be met, but in order to do so there must always be an underlying support mechanism (unless users decide to run OSI applications over TCP/IP with something such as ISODE). The usage of OSI application services, as well as product availability will drive requirements in the NSN backbone for OSI end-to-end service support.

The NSN backbone routers will support forwarding of ISO 8473 packets in 1990. At this time, testing of upper-layer applications will be feasible. Vendor software release with ISO 8473 forwarding capabilities is expected in 1990. Operational support of ISO 8473 can be accomplished on the NSN backbone when the following items are resolved: (1) the GOSIP Version 2 NSAP address structure is defined, (2) routing domain and area boundaries are designated, (3) an administrative authority portion of the NSAP address is received from GSA, and (4) a NASA-wide procedure is developed for further registering and disseminating the remaining portions of the NSAP address to NASA network administrators and then to users.

These issues are being coordinated with SPAN's efforts to transition to Phase V because many of the topics overlap.

Until there is an OSI standard implemented for dynamic routing, either static routing or some other interim mechanism a vendor may have for dynamic intradomain or inter-domain routing will be used.

The forwarding of ISO 8473 packets is limited because a complete end-to-end service via OSI protocols is not yet available in vendor products. Therefore, this first stage is expected to be limited. It provides a limited user-base access across the backbone for those who wish to communicate via ISO 8473 to other users. As the size of the user base increases, the need for a complete OSI protocol stack increases as well.

6.2 OSI and SPAN

Since 1980, SPAN has grown from a small, private DECnet network of six nodes to over 7,000 nodes today. SPAN connects to other DECnet networks, such as ESNET/DECnet, European-SPAN, and European-HEPNET. These combine to represent NASA and DOE agencies in the United States, European Space Agency (ESA), and major research and technical centers throughout Europe. This has resulted in a DECnet Internet of more than 20,000 DECnet nodes.

Accompanying this growth are problems with the limited architecture of DECnet Phase IV which includes network addressing limitations.

DECnet Phase IV is the current version of the networking technology in use on SPAN. SPAN has used DECnet Phase III (1981-1984) and DECnet Phase IV (1984-present). The next version of DECnet (Phase V) is expected to be available in late 1990.

The DECnet Phase V implementation includes some OSI protocols, with interim solutions for the as yet nonstandardized OSI protocols. DEC has made a public commitment to conform to future OSI standards as they evolve.

6.2.1 Issues of the Existing DECnet Internet

DECnet Phase IV is limited to 1,023 nodes in each of 63 areas, for an architectural maximum of 64,449 nodes in the world-wide network. The practical limit (due to the current topology and circuit bandwidth) is lower, and for optimal routing, response has proved to be up to 300 nodes per area.

The DECnet Internet, consisting of several networks, including US-SPAN, European-SPAN, ESNET/DECnet, and European-HEPNET, now contains in excess of 20,000 nodes. In 1985, the cooperating network managements agreed to limit the internationally recognized areas to 46, allowing continued operation of multiple local subnetworks in DECnet areas 47 to 63 to alleviate local site constraints. Many internationally recognized areas (those from 1 to 46) are full or very nearly full, thus limiting the growth of the overall network.

At last count, more than 7,000 nodes were identified as occupying the SPAN subset of internationally recognized DECnet areas, and growth in the past few years has doubled the size of the network each year. It is clear that it is architecturally impossible to double the size of the network for more than another year. An even more pressing issue, however, is that utilizing existing address space has additional constraints on

how the remaining addresses can be used. Addressing limits and the subsequent inability to grow have been recognized as the primary reasons behind plans for transitioning from DECnet Phase IV to Phase V protocols.

A direct consequence of having so many nodes in areas and in the network is the observed behavior of the routers and the routing. There is a large amount of routing information which can degrade user-perceived performance.

The biggest impact of the routing behavior in the DECnet Internet is evidenced by the fact that Phase IV has no concept of routing domains. Therefore, all areas in the world know how to get to all other areas in the world dynamically. This means that there is no shielding of routing information, and should one site inadvertently introduce a duplicate area into the network, the result is that the routing information to the original area is corrupted, causing the network to partition. Partitioning is perceived by the user as loss of connectivity.

The only recourse for repairing the partition is for network management to manually identify the source of the problem and disconnect the errant site until the local addressing is repaired. OSI, and hence Phase V as well, introduces routing domains, which permit complete shielding of internal routing messages from propagating to the DECnet Internet. Local site routing and addressing assignments can be carried out without the need for international agreement.

6.2.2 Phase V - Phase IV Interoperability

DEC plans to provide interoperability between Phase IV and Phase V systems. In order to minimize impact to users, SPAN will depend on Phase V's interoperability with Phase IV (also referred to as backwards compatibility).

Interoperability between Phase IV and Phase V nodes is restricted to within a routing domain. This means two things:

(1) A node upgrading to Phase V will need to use a Phase IV-compatible address if it has transparent interoperability requirements with other Phase IV nodes, and

(2) Designating routing domains could become an issue.

Designating a very large routing domain could become an issue if the size is large enough to cause problems with the intradomain link state routing protocol, analogous to the problems now viewed with Phase IV routing. It is estimated, however, that the entire DECnet Internet in areas 1-46, along with associated level-2 routers, could reside in a single routing domain with room for growth. Also, the use of a single routing domain during transition of the entire Internet is not being planned. Rather, SPAN will initially adopt a single routing domain for its transition to facilitate transparent interoperability, and as transition progresses, SPAN will eventually split into separate routing domains consistent with the final goals of OSI networking for NASA. (See App. D, Routing Domains.)

6.2.3 Naming and Directory Service Issues

One of the prerequisites for DECnet Phase V is the installation of the Digital Network Architecture Naming Service (DNANS) (ref. 15) in the network. DNANS will provide a distributed network database, replacing the remote node databases that

now exists in Phase IV. DNANS will provide a wide area network service, with up-to-date information on addressing and other information required to establish network connections. DNANS must be installed before Phase V protocols can be used.

ESNET/DECnet has proposed a DECnet naming convention that SPAN and the DECnet Internet intend to adopt.

The naming service, if installed only at NASA/SPAN centers, can be used by Phase V network nodes at nonbackbone local sites over the wide area network connection. However, for performance considerations, installing a DNANS server at large nonbackbone local sites would optimize performance.

6.2.4 DNANS Interoperating with X.500

Where DNANS is the DECnet Phase V Directory Service, X.500 is expected to be the International Standard directory service with products available by 1992. By adopting DECnet DNANS, NASA raises the issue of how this will affect a later transition to the International Standard for directory service. DEC, however, has publicly committed to providing an X.500 interface for DNANS when X.500 is fully developed. This is an issue that needs additional review.

6.2.5 Phase V Routing and Addressing

DEC has taken the lead in designing the Intradomain routing Protocol, which is currently in the process of becoming an International Standard. This protocol is the Intermediate System to Intermediate System (IS-IS) (ref. 16). Even though it is not fully standardized yet, the Phase V products will include it, and hence the dynamic routing of ISO 8473 packets. The added benefit is that this routing protocol is available now and is also likely to become an OSI standard.

Under IS-IS, there are new aspects to routing. In addition to the area, there will be another level of addressing, called the routing domain. According to GOSIP Version 2.0, within an area there are 6 octets that can be used as end system node identifiers, resulting in a theoretical limit of 2^{48} end systems per area. However, a more practical limit is 4,000 to 10,000 end systems. Similarly, a routing domain is interpreted by using 13 octets, resulting in a theoretical limit of 2^{104} routing domains, yet the realistic limit will be much smaller. Regardless of the practical limit, this provides a very large amount of address space.

One important item to note is that DEC does not support transparent interoperability between Phase IV and Phase V nodes in different routing domains. Phase IV nodes will only be able to communicate with Phase V nodes if the Phase V node has a Phase IV-compatible address (i.e., an area less than 64, and a node less than 1,024) and they are within the same routing domain. In the beginning of transition from Phase IV to Phase V, most Phase V nodes will have Phase IV-compatible addresses. The technique used to effect the transition will permit limited address relief. However, extensive use of new addresses will be delayed. This will be true until either a method is developed to ensure Phase IV to Phase V transparency, or the Phase IV to Phase V compatibility requirement is sufficiently reduced, which will happen as transition progresses.

7.0 POSSIBLE PATHS FOR OSI INTEGRATION IN NSI

There are two ways to integrate OSI into the existing NSN and SPAN networks. This section analyzes these approaches. Within each approach there are variations, however, only the overall implications are examined here.

The two approaches NASA is considering for OSI integration are:

(1) SPAN and NSN each go to OSI separately:

SPAN and NSN each integrate OSI separately maintaining separate backbones and operational management throughout most of the integration period. SPAN uses DECnet Phase V products and NSN uses nonspecific commercial vendor products. As integration of both networks progresses and true interoperability becomes possible, the networks will merge backbones and management structures. This results in a final unified network and protocol stack for NASA science users.

(2) SPAN and NSN combine and go together to OSI including DECnet Phase V.

SPAN and NSN combine backbone circuits and operational management now, and together integrate OSI with DECnet Phase V and other commercially available products as they become available. As the integration of OSI protocols progresses, hosts on NSN and SPAN will become interoperable at much the same time. The final NASA Science Internet is the same as proposed by (1).

It is important to realize that the two approaches outlined above will result in the same final structure for NSI. However, the approach chosen must provide the best path for maintaining existing user services while setting the stage for the integration of OSI protocols.

The rest of this section presents the goals for the final structure of the NSI, followed by an analysis of the paths to reach these goals. The analysis includes the most important technical issues, their pros and cons, and the schedule and cost estimates of each path to the OSI protocol suite.

7.1 Resultant NSI Structure and Goals

It is necessary to outline what the goals are for a complete OSI integration before a technical analysis of approaches is carried out. The NSI network, after integration, is envisioned as supporting a full GOSIP-compliant OSI stack using multivendor products under one central engineering and network management authority. It will be able to connect and interoperate with other OSI networks at this time.

Consistent network addressing, routing, naming, and multivendor interoperability are important issues that are clearly defined as goals of the NSI. In addition, responsive network management is an important aspect of maintaining the resultant network.

7.2 NSI/OSI Addressing

After GSA guidelines are implemented, NASA is expected to receive an "administration authority" identifier, which is used in all NASA NSAP addresses, and from which over 65,000 routing domains may be defined. It is necessary to use only one routing domain on a single Ethernet-based local area network. Therefore, NSI management must work closely with other NASA network managers to ensure that multiple routing domains do not appear indiscriminately on local site networks.

7.3 NSI/OSI Routing

Setting routing domain boundaries and circuit metrics to define these boundaries will control NASA traffic on the NSI as well as eliminate transit traffic from non-NASA sites destined for other non-NASA sites. It will be an NSI management task to maintain these links and effect changes to maintain network operations under OSI.

It is currently anticipated that the NSI backbone will occupy a single routing domain, thus isolating all its routing information from local site networks. Sites served by the NSI backbone will similarly be in separate routing domains. This is especially necessary when the site is connected to other backbone networks. Using separate routing domains completely isolates local site routing problems, if they occur, from the rest of NSI or other wide area networks. Setting circuit metrics on routing domain boundaries with static links will be the method used to control traffic over the backbone, allowing a form of "policy-based routing."

Using multiple domains in this way has its pros and cons. On the pro side, a form of policy-based routing can be enforced. With one large routing domain, if a partition occurs, it could result in backbone transit traffic traversing a local site network. With a routing domain boundary between the backbone and local site, this is easier to avoid. In addition, local site routing problems that result in erroneous routing information will be secluded from the backbone. On the con side, since there currently is no dynamic interdomain routing, there will be static links at the routing domain boundaries. This will cause disruption due to the need to have manual intervention to reroute traffic in case of circuit failure. Furthermore, the information in routing tables as well as in routing update messages will increase in size as the number of routing domains increases.

7.4 NSI/OSI Naming

NSI OSI will use X.500 standard naming guidelines and recommendations as they evolve in the GOSIP standard. Registration of NSI names will be administered by NSI management. Name servers will be deployed at each NSI OSI center.

7.5 NSI/OSI Network Management

A single network structure will result in unified network management. NSI is expected to provide an operational network management structure using standard OSI protocols as they become available to maintain the backbone and local site connectivity. NSI network management can also be expected to provide name and address registration.

7.6 Option 1: SPAN and NSN Integrate OSI Separately

In this scenario, SPAN and NSN maintain their existing backbones while integrating OSI protocols separately. SPAN will integrate DECnet Phase V into the existing network. As the OSI standards evolve, SPAN will incorporate them.

NSN will gradually provide OSI services as they become commercially available. NSN will provide interim standard protocols that will enable an operational network. For example, as an interim management TCP/IP protocol, work is currently under way for the Simple Network Management Protocol (SNMP) (ref. 17) to include OSI management capabilities.

SPAN and NSN would then merge their backbone routers and network management structure as soon as it is technically feasible.

Schedule:

Transition of the bulk of SPAN, including SPAN local sites, from DECnet Phase IV to OSI protocols is targeted to take at least two years from the initial transition of the SPAN backbone. SPAN will begin to carry ISO 8473 on the backbone in 1990 or early 1991, enabling connected sites that support Phase V to use the backbone for OSI traffic.

NSN will begin limited deployment of OSI ISO 8473 in the NSN routers in 1990 or early 1991. This will enable end systems to use the backbone for OSI traffic. The dynamic IS-IS intradomain routing protocol will be used as soon as it is available in commercial routers, which is estimated to be in late 1991. Additional deployment of OSI products is largely dependent on the market trends and end system OSI usage and requirements.

Costs:

Table 3. Cost of Beginning the Incorporation of OSI Products into the SPAN and NSN Backbones ($ 000s)

	FY91	FY92
SPAN Required Items:		
Operations*	90.7	90.7
Backbone Transition	158.1	127.3
SPAN Desired Items	94.4	42.5
NSN ISO 8473 Software	15.0	0
	$358.2	$260.5

** The cost for SPAN operations is a required upgrade regardless of the OSI integration.*

Table 3 estimates only the costs for beginning the incorporation of OSI products into the SPAN and NSN backbones. It does not include the local site or European site costs. (For a more detailed estimate of the Phase V integration cost, including user

site costs, see App. E.) The cost for the NSN backbone is only for software in the intermediate systems (backbone routers) to forward ISO 8473.

Pros:

(1) Begin alleviating SPAN's addressing problem:

Some alleviation of the address limitation is possible: it is estimated to be on the order of hundreds of nodes during the initial transition period.

Address relief will be available in the following cases:

- New Phase V nodes that do not interoperate with any other Phase IV nodes (~200). If transparent interoperability is a requirement, new Phase V nodes must be assigned Phase IV addresses. All other nodes must continue to maintain their Phase IV address until the requirement for backwards compatibility with Phase IV nodes is no longer required.

- There is a set of Phase IV area numbers that have been reserved for transition by the consortium of DECnet networks (SPAN, HEPNET, European-SPAN, and European HEPNET). These are to be used as the core Phase V areas. These areas can provide some address relief until OSI addressing can be used more extensively.

(2) Supports the DECnet Network Management Listener:

The DECnet Network Management Listener (NML) protocol will be supported for Phase IV across the backbone, since DEC routers will be used. As DECnet Phase IV is replaced by Phase V, support of NML will become a less significant issue. In addition, DEC will provide Common Management Information Protocols (CMIP) for DECnet Phase V. CMIP will form the basis for future network management of OSI networks.

(3) Provides interoperability between Phase IV and Phase V:

By using DEC routers across the backbone, as opposed to using non-DEC multiprotocol routers, the required interoperability between Phase IV and Phase V end system nodes within a routing domain is assured. DEC routers have partially dual stack architectures (Phase IV and Phase V) that transparently provide interoperability between Phase IV and Phase V nodes.

(4) Dynamic Intradomain Routing:

DEC has implemented intradomain dynamic routing, IS-IS, in Phase V. IS-IS is not yet an OSI standard, but it is currently a Draft Proposal in the ISO/IEC standards organizations. It is anticipated that IS-IS will become fully standardized in 1991.

Cons:

(1) Problems with asymmetric routing of traffic

A technical problem with NSN and SPAN both forwarding ISO 8473 packets is asymmetric routes. Asymmetric routes can cause operational management problems.

In this scenario, both NSN and SPAN backbones connect to the main NASA centers where they both will be carrying ISO 8473. Where traffic is destined to another NASA center with both NSN and SPAN ISO 8473 connections, the traffic may go out over one backbone and return over the other. Only by careful configuration of the routers based on policy decisions on both ends can symmetric routes be assured. Since SPAN and NSN both serve the same community, making policy decisions is not justifiable. Furthermore, the local sites may need to physically separate the end-system nodes into NSN and SPAN groups with different addressing so that the same address space is not on a shared Ethernet. This is clearly unrealistic.

(2) Network management protocols not yet standardized:

The network management protocols used by SPAN and NSN will be different. NSN may use the TCP/IP Internet SNMP standard for management of OSI, while SPAN will rely on NML for DECnet Phase IV and will use CMIP for DECnet Phase V. The use of multiple network management tools can lead to some confusion.

(3) DEC routers do not support multiple protocols:

DEC routers do not currently support other standard protocols. This limits their versatility.

(4) DEC routers do not support multiple T1 interfaces:

The DR2000 that DEC provides as a router does not support more than one T1 interface per router. Due to the anticipated increase in user requirements for bandwidth, the DEC router will be a limiting factor when engineering a backbone site with multiple high-speed links. This also limits future engineering of the backbone using higher speed links with a topology that provides redundant paths on the backbone. Having only one connection from a router to the backbone results in a tendency towards a star topology with no redundant paths. Another scenario is to use two DEC routers, however, traffic transits the site as well as incurs an extra hop on the backbone.

(5) Other limitations of single-vendor DEC router products:

Most DEC routers require VAX/VMS* load hosts to provide downline load and upline dump services, and cannot be downline loaded from a synchronous interface.

Finally, single-vendor solutions are not the intent of OSI.

**VAX/VMS is a trademark of the Digital Equipment Corporation*

(6) Limited use of OSI addressing initially:

Initially with Phase V there will only be limited use of the new OSI addressing. This alleviation is the driving factor for transitioning to Phase V as soon as possible. See item (1) under *Pros*, section 7.6, for an explanation of the limited address capabilities during the transition period.

Issues to Resolve:

(1) Unified network management structure:

Plans must be developed to provide a unified network management structure for the resultant NSI.

(2) Routing domain size:

Designating routing domain boundaries is an issue. With this option there must be careful coordination between the separate SPAN and NSN backbone design efforts. (See App. D for more details on routing domains.)

7.7 Option 2: SPAN and NSN Jointly Integrate OSI Including DECnet Phase V

The NSN and SPAN backbones are combined by using the same circuits with multiprotocol routers forwarding IP, Phase IV, and ISO 8473 traffic between the NASA centers. The Phase V protocols include the use of ISO 8473 at the network layer. Some user sites requiring support of both TCP/IP and DECnet Phase IV are already connected to NASA using multiprotocol routers.

This analysis focuses on backbone issues.

Schedule:

The schedule for transition of the bulk of SPAN, including SPAN local sites, from DECnet Phase IV to OSI protocols is difficult to estimate. The solution to the Phase IV to Phase V compatibility requirement, which is yet to be resolved, may impact the schedule.

The NSN multiprotocol routers, in this scenario, will carry operational ISO 8473 traffic as well as DECnet Phase IV traffic in 1990. This will enable end systems to use the backbone for OSI traffic, TCP/IP traffic, and DECnet Phase IV traffic. Dynamic IS-IS intradomain routing protocols will be used as soon as they are available in commercial routers, which is estimated to be in late 1991. Additional deployment of OSI products is largely dependent on the market trends and end-system OSI usage and requirements.

Costs:

Table 4. Cost of Incorporating OSI Products in the Combined SPAN and NSN Backbones ($ 000s)

	FY91	FY92
SPAN Required Items:		
DNANS for NASA centers	158.1	127.3
SPAN Desired Items	94.4	42.5
NSN ISO 8473 Software	15.0	0
Multiprotocol Routers	*	*
DEC Routers for Interoperability	*	*
	>$267.5	>$169.8

** The number of multiprotocol and DEC routers is unknown at this time; information to be supplied by NSIPO.*

Table 4 estimates the cost for incorporating OSI products in the combined SPAN and NSN backbones only. It does not include the local site or European site costs. (For a more detailed estimate of the Phase V integration cost, including user site costs, see App. E). The combined NSN-SPAN backbone cost is for intermediate systems (backbone routers) forwarding ISO 8473. This table does not include the costs of circuits. It also does not include additional interoperability gateways for Phase IV to Phase V that may be required at the local sites.

Pros:

(1) No asymmetric routes:

Asymmetric routes are avoided, since there will only be one NSI external connection into NASA local sites. See Option One (section 7.6) *Cons* (1), for additional details on the implications of asymmetric routes.

(2) Multiple T1 interfaces are supported:

Instead of using DEC routers, NSI will use higher performance routers capable of supporting multiple T1 interfaces. See Option One (section 7.6) *Cons* (4) for details.

(3) Multiprotocol service to selected sites:

With multiprotocol routers, selected sites are capable of meeting their requirements by the use of a single link. Some sites may gain additional protocol connectivity by moving up to the multiprotocol approach.

Cons:

(1) Non-DEC routers do not support the DECnet Network Management Listener:

The DECnet Network Management Listener (NML), will not be available across the backbone for Phase IV. The lack of NML will result in near-term reorganization of the network operations and management procedures that are currently in place.

(2) Interoperability between Phase IV and Phase V:

Interoperability between Phase IV and Phase V using non-DEC routers is not currently supported. Several potential solutions have been suggested.

(3) Static ISO 8473 routing:

Until the IS-IS intradomain routing protocol becomes an International Standard and is implemented in the NSI multiprotocol routers, all intradomain routing must be done statically. This will result in manual routing configurations, which will become an increasing problem as more and more circuits start requiring ISO 8473 support. It is anticipated that the IS-IS routing protocol, which is a Draft Proposal in the standards organizations, will be an International Standard in 1991, at which point an implementation will likely be made available by vendors who support ISO 8473 forwarding capabilities.

Issues to Resolve:

(1) Interoperability between Phase IV and Phase V:

Solutions for interoperability between Phase IV and Phase V end systems across the backbone require further investigation.

There are several questions that need to be addressed, such as: are interoperability gateways between Phase IV and Phase V nodes available, and if so, will they provide the necessary end system user support required? The use of DEC routers to perform address translation has been introduce as a potential solution, however, further research and testing is required.

(2) Operations and management structure:

Plans must be developed to provide a unified network management structure for the combined SPAN and NSN backbones which supports 24-hour-a-day, 7-day-a-week service.

(3) Routing domains:

Designating routing domain boundaries is an issue. Since the backbones are consolidated, coordination between NSN and SPAN backbones is not required. (See App. D.)

Appendix A

OSI Standardization Procedures

OSI standardization and development is a multinational endeavor achieved through various organizations such as the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), which has a Joint Technical Committee (ISO/IEC). In addition, the International Telegraph and Telephone Consultative Committee (CCITT) is involved.

Within these organizations, standards are developed with the anticipation of becoming International Standards. These are presented to the ISO/IEC members for formal evaluation and balloting by each participating organization. As with all standardization procedures, final consensus can be a lengthy process. OSI has been under development for approximately 12 years.

The forum representing the United States as a voting member is the American National Standards Institute (ANSI). ANSI casts the U.S. vote at the ISO/IEC meetings. The participants within ANSI largely represent vendors, however, there are also government agencies such as NASA, the National International Standards Bureau (NIST), and other organizations as well.

The CCITT produces "Recommendation" documents which are combined every four years into a set of specifications. Much of the work that is produced in these Recommendations are included in the OSI standards (e.g., X.25 and X.400). The Recommendations that are developed over a four-year cycle compose what is referred to as "colored books" (e.g., the Blue Book contains Recommendations produced between 1984 and 1988). Each document in a colored book has an identification letter, number and date. For example, the X.25 (80) and X.400 (80) specifications are part of the Red Book produced in the 1980 to 1984 time frame. A revision to X.25 may then produce a new Recommendation X.25 (88).

The path a document takes in order to achieve the status of an International Standard is as follows:

(1) The document is proposed by a ISO/IEC member as a "Working Draft" (WD). It is given a number and a committee is assigned to review it.

(2) The committee appointed makes a decision as to whether the WD should progress to the next step. If so, the document becomes a "Draft Proposal" (DP).

(3) After at least six months, the DP is voted upon by the ISO/IEC members. This step may be repeated once to incorporate comments. If it is still not agreeable to a majority of the voters, then the DP is abandoned or restarted from the beginning.

(4) If passed the document becomes an "Draft International Standard" (DIS). After another six-month waiting period, it is voted upon again.

(5) If passed again, the document becomes an International Standard.

The ISO/IEC members may vote on the documents in one of four ways: 1) no, with reasons, 2) no, with stipulations that if met will change the vote to a yes, 3) yes, with comments, and 4) yes, with no comments.

Standards conformance testing is done on vendor OSI products to ensure correctness and interoperability. The details and schedule for accomplishing this task are currently being developed.

Appendix B

Network Service Access Point Structure

The Network Service Access Point (NSAP) is used to uniquely identify a node without relying on media-specific addresses.

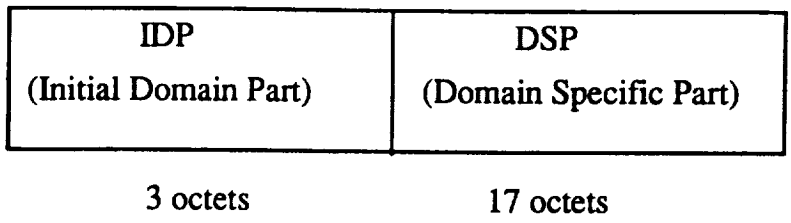


Figure 7.- The Initial Domain Part (IDP) and the Domain Specific Part (DSP)

Figure 7 shows the Initial Domain Part (IDP), which is assigned by the ISO/IEC, and the Domain Specific Part (DSP), which has a structure defined in GOSIP Draft Version 2.0 (ref. 18).

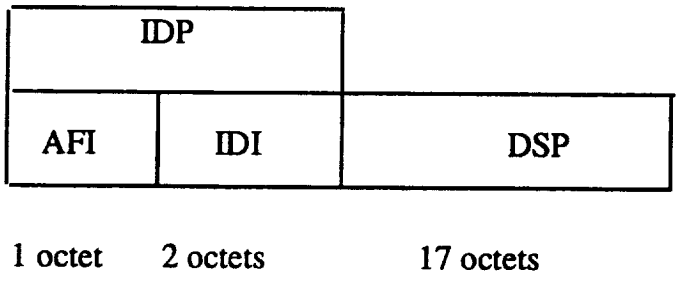


Figure 8.- Components of the IDP

The IDP portion is made up of the Authority and Format Identifier (AFI) and Initial Domain Identifier (IDI) fields. The AFI indicates how the packet is to be interpreted. The AFI for GOSIP NSAP addresses is 47, and the IDIs owned by the United States are 4, 5, and 6. The ISO/IEC has given the numbers 4 and 5 to NIST. NIST owns 4, which is for OSINET, as well as 5, which is the U.S. government. In addition, NIST applied on behalf of DOD to obtain an ICD, 6, which now belongs to DOD.

IDP		DSP						
AFI	IDI							
47	0005	Ver.	Admin. Author.	Rsrvd	Routing Domain	Area	End Sys.	Nsel
1	2	1	3	2	2	2	6	1

# of octets

Figure 9.- Composition of the DSP Portion

Figure 9 shows the composition of the DSP portion as defined by the draft version of GOSIP Version 2. It is still under consideration and is expected to become standardized in 1990. This diagram is the DRAFT version and could potentially change.

Each administrative authority identification will be registered and disseminated by the Telecommunications Customer Service Division in the GSA. The remaining address block will be handed out by the administrative authority. For example, NASA has, or soon will have, have a specific administrative authority number.

Appendix C

U.S. GOSIP

The OSI protocol suite offers a wide range of options and further refinements within options, some of which are specifically incompatible. Careful consideration must be given when making decisions on which OSI features to choose in order to ensure compatibility among the numerous vendor products running in a particular network. The Federal Information Processing Standard (FIPS) 146 Publication on the Government OSI Profile (GOSIP) (ref. 1), specifies OSI options and refinements to use within the United States.

The FIPS 146 for GOSIP Version 1 became effective in February 1988 and will become a requirement, where applicable, after an 18-month grace period starting in August 1990. The FIPS 146 Draft Version 2 (ref. 18) is expected to become effective in June of 1990 and a requirement 18 months later.

This profile specifies a particular subset of the OSI protocols. GOSIP is important in that it identifies an OSI subset for the U.S. government, and hence vendors in general which will facilitate compatibility among OSI networks. There is, however, some vagueness and confusion as to what the GOSIP actually means for the procurement process within government agencies for existing operational networks.

GOSIP is intended for procurements of new network services and for major network service upgrades (e.g., electronic mail is a network service). What actually constitutes a "major network service upgrade" is a grey area that is not explicitly defined in the FIPS publication. It is up to each agency to decide what a major network upgrade is. When an existing network will not easily interoperate with OSI protocols or when there is a requirement that OSI cannot meet, then GOSIP may not apply. In cases where OSI does not apply, a formal waiver is not required to bypass citing and acquiring OSI protocols.

The OSI Division within the NIST organization is responsible for writing the GOSIP document. The technical implications of the numerous OSI options that are available are considered for inclusion in the profile. The OSI Implementors' Workshop produces an evolving document called the Stable Implementors' Agreements (ref. 19). GOSIP is based on these agreements and is then distributed for comments before a final version is released. Members of the OSI Implementors' Workshop are mainly vendors. However, other representatives such as from Government agencies attend as well.

As a reference to GOSIP and OSI terminology and meanings, the *Government Open Systems Interconnection Profile Users' Guide* (ref. 14), is recommended. Each version of GOSIP will be followed shortly thereafter with a new revision of the GOSIP *Users' Guide*.

C.1 Waivers to GOSIP

In some cases a waiver may be required. The GOSIP waiver process requires the approval of an agency head or an designate thereof. The waiver process will be complicated and should probably be avoided whenever possible. In any case, it is essential that NASA establish a procedure for the waiver process prior to August 1990.

There may be cases where GOSIP simply does not apply. The network administrator is responsible for deciding under which circumstances GOSIP may or may not apply. In cases where GOSIP does not apply, the waiver procedure is not required.

C.2 Current and Future GOSIP Specifications

As new OSI protocols become standards and are commercially available, the GOSIP document is updated to reflect and include these changes as necessary.

This section gives an outline of the features in GOSIP Version 1 and the GOSIP draft of Version 2 (see fig. 10). Anticipated additional features in future versions of GOSIP (3 and 4) are outlined as well.

(1) GOSIP Version 1 (effective February 1988; required August 1990)

- o Physical and Data link Layers protocols (X.25, IEEE 802.3, 802.4, 802.5)
- o Connectionless Network Service (ISO 8473)
- o Connection-Oriented Transport Service (TP4)
- o File Transfer, Access, and Management (FTAM)
- o Message Handling Systems (MHS) [Based on X.400 (84) CCITT Recommendation]

(2) GOSIP Version 2 (estimate effective date in 1990)

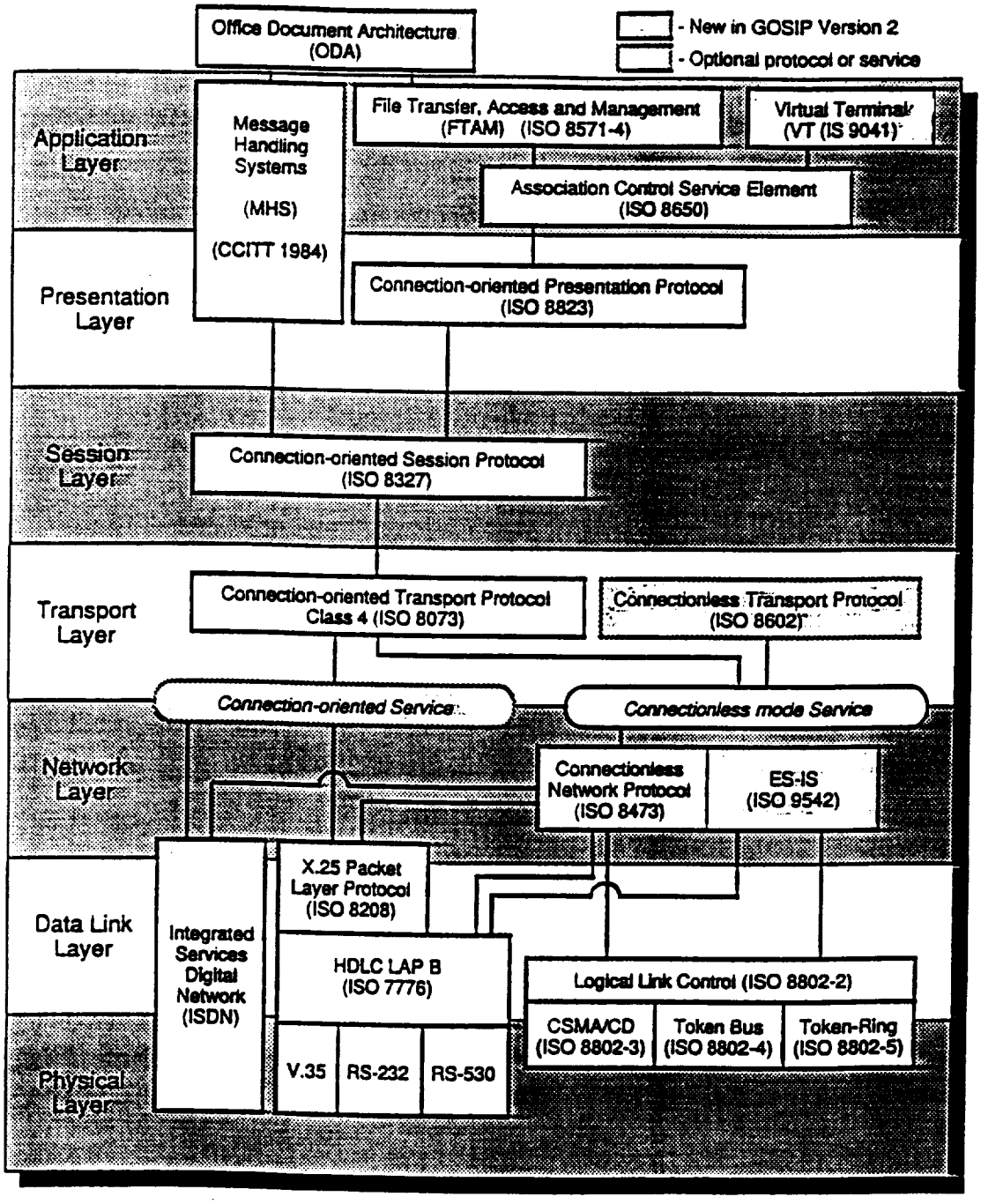
- o Virtual Terminal (VT) Service
- o Office Document Architecture (ODA)
- o Connectionless Transport Service (CLTS), optional
- o Connection-Oriented Network Service (CONS), optional
- o Integrated Services Digital Network (ISDN)

(3) GOSIP Version 3 (effective date unknown)

- o Directory Services
- o Virtual Terminal Modifications (page and scroll profiles)
- o MHS Extensions [CCITT Recommendation X.400 (88)]
- o File Transfer, Access, and Management (FTAM) Extensions
- o Fiber Distributed Data Interface (FDDI)

(4) GOSIP Version 4 (effective date unknown)

- o Transaction Processing
- o Remote Database Access
- o Electronic Data Interchange (EDI)



**This diagram is courtesy of the Systems and Network Architecture Division of the National Institute of Standards and Technology under the Department of Commerce.*

Figure 10.- GOSIP Version 2.0 OSI Architecture.

Appendix D

Routing Domains

ISO 8473 packets are routed by using portions of the NSAP address. GOSIP Version 2 defines fields in the NSAP, such as the administrative authority, routing domain, and area that relate to the routing (see App. B, Network Service Access Point Structure). Intermediate System (IS) routers are required to route GOSIP as well as non-GOSIP structured ISO 8473 packets, yet the GOSIP Version 2 structure provides a hierarchical structure that is intended to facilitate both interdomain routing and address administration. The high-order part of the NSAP up to, but not including, the area field is considered the routing domain identification (note that there is also a specific routing domain field). A routing domain is composed of areas, and areas contain a collection of end-system user machines. Dynamic Intradomain routing will be accomplished within a routing domain by using the IS-IS protocol. IS-IS is currently a Draft Proposed (DP) International Standard.

The GSA is registering and disseminating Object Identifiers to government agencies with the expectation that later (when GOSIP Version 2 is a FIPS) the GSA will bind the usage of these IDs to the administrative authority field. The remaining address block will be allocated and registered by the agency that acquired the administrative authority identification. Initially it is expected that each government agency will assign all NSAP addresses under one administrative authority number.

Full standardization of Intradomain IS-IS is expected within one year. Work on a dynamic Interdomain IS-IS is beginning, but no results are anticipated until 1995.

Interdomain routing will be done statically until there is a dynamic interdomain protocol standard available. Dynamic routing within a routing domain is carried out at two levels: within areas (level 1 routing) and between areas (level 2 routing).

D.1 Considerations

There are several things to consider when designating boundaries for the domains as well as areas.

Dynamic routing can be utilized within a routing domain. However, when traversing a routing domain boundary, static routes must be used, since interdomain dynamic routing is not available at this time. Static routing can be a disadvantage when links go down and rerouting of packets is required. In addition, static routing is more time consuming to manage since it requires more manual configuration in the routers compared to automatic reconfigurations accomplished by dynamic routing. It has been argued, however, that error checking and policy filtering is required at network boundaries in any case.

The level of trust at a network boundary needs to be determined by the network administrator on each side of the boundary. For example, the trust level typically declines when crossing from one network to another where each network is managed separately (i.e., control of each network's routers is under different administration). This is an issue because routing can be complicated, and misconfigured routers can cause severe problems for other connecting networks. There are precautions that can be taken to ensure protection from misconfigured routers, and establishing a routing domain boundary may facilitate precautionary measures. There is some protection at

the area boundary. However, this may not be sufficient protection, especially if the routing domain partitions. A routing domain boundary may provide an additional wall for enhanced error-checking capabilities that facilitate assurance that one network does not cause a problem, such as sending incorrect routing information. The need to control routing within a network, for policy or other reasons, could potentially result in the need to designate a separate routing domain.

A routing domain provides a very large amount of address space, yet it may need to be designated for other reasons such as policy and protection. In order to help control a potential explosion in the number of designated routing domains, establishing routing domains should be considered carefully.

If there is in fact a large number of routing domains within a single administrative authority, some type of information collapse is necessary to keep the amount of routing table information under control. Anticipation of this problem has led to the consideration of assigning an administrative authority number to the regional networks (in addition to the agency networks). Having each regional use an administrative authority will allow a route to be set pointing to all the routing domains within the administrative authority. Conversely, if there was a common administrative authority, e.g., between NSFNET and all the regionals, there would be a routing entry for each routing domain (instead of each regional) resulting in an increase in routing information.

Another item to consider is that one of the largest deployments of OSI-based networking technology will soon be DECnet's Phase V. Maintaining interoperability between DECnet Phase IV and Phase V will be required during the transition period from Phase IV to Phase V. There are several ways to achieve compatibility between Phase IV and Phase V:

(1) Translate addresses between Phase IV and Phase V. This is the basic tool for Phase IV to Phase V compatibility.

(2) Use Phase IV addresses over different routing domains during the transition (i.e., the currently designated Phase IV areas may fall into different routing domains, especially when international boundaries are crossed).

It is anticipated that the transition period will extend over a 2- to 3-year duration. Although DEC provides interoperability between Phase IV and Phase V nodes within a routing domain, interoperability between routing domains may be difficult. There have been some proposed solutions that are likely candidates to be used in a few select cases. Some special routing domain boundaries will be required during transition to facilitate interoperability between Phase IV and Phase V nodes. However, it is recognized that this could impact the rest of the community of non-DECnet users, since the way they designate routing domains may not fit into the way they have already been defined. Since the transition period will continue for several years, the design should be as general as possible to include solutions for non-DECnet as well.

D.2 National Backbones

Backbone network carriers such as NSN, ESNET, and NSFNET will define a unique routing domain for each of their respective backbone networks. In addition, they will have an administrative authority that is unique to their particular government agency. The backbones connect to other networks including regionals and local site

networks. Local site networks could consider, when feasible, adopting their backbone's routing domain.

D.3 Regionals

It may be desirable for each regional to define its own routing domain as well as its administrative authority. In the event of rapid growth in the number of routing domains, having each regional network have its own administrative authority will facilitate routing table information collapse.

D.4 Local Sites

When defining a routing boundary, the characteristics of a local site should be considered. The local site may vary in size and topology as well as in its relation to the backbone carrier. It may be a large site with multiple external backbone carriers, or it may be a site with only one direct connection to a backbone or regional network. When a site has multiple external connections, establishing its own routing domain may be desirable. If it is a site with only one external carrier, then it should consider being an area that is part of the external carrier's routing domain.

Appendix E

SPAN Phase V Transition Costs

There is some DEC hardware and software that will become obsolete under Phase V. Therefore, it will be necessary to purchase some new equipment and to allocate funding for the Phase V transition: for example, all PDP-11 systems, DECSAs, DEQNAs and DMV11s for VAX Q-Bus systems, and DMR11s for VAX Unibus systems. DEQNAs must be upgraded to DELQAs, DMV11s to DSV11s, DMR11s to DMB32 or DSB32 (BI only), or DR2000, DECSAs, and PDP-11 routers to DR2000. PDP-11 hosts should be downgraded to act as end nodes in order to function in a Phase V network.

The following tables provide details on the costs for the Phase V transition, including information for a separate Phase V backbone.

Table 5. Overall Cost Estimate for the SPAN Backbone, Local Site, and European Expenses ($ 000s)

	FY91	FY92
Required:		
(SPAN Operations)	90.7	90.7
(P5 Trans-SPAN BB)	158.1	127.3
(P5 Trans-NASA Sites)	68.9	68.9
(P5 Trans-Tail Sites)	321.5	321.5
(P5 Trans-Int'l)	80.6	80.6
Desired items	94.4	42.5
DEC consultant	180.0	0
Total	$994.2	$731.5

Table 6. SPAN Operations Upgrade: Necessary Replacement of Obsolete, Unreliable Routing Equipment at NASA/SPAN Routing Centers.

Item	Number Needed	GSA Cost ($ 000s)	Potential Breakout over FY91 ($ 000s)	Potential Breakout over FY92 ($ 000s)
DEMSA	16	9.96	77.4 (8)*	77.4 (8)*
X25 DEMSA	2	13.3	13.3 (1)*	13.3 (1)*
Total			$90.7	$90.7

**Indicates the number of units to be purchased for the specified price.*

Table 7. Required Items for SPAN Backbone DECnet Phase IV to DECnet Phase V Transition

Item	Number Needed	GSA Cost ($ 000s)	Potential Breakout Over FY91 ($ 000s)	FY92 ($ 000s)
DNANS s/w License	19	3.3-4.5	42.9 (11)*	31.2 (8)*
DNANS h/w VAX 3100 w/disk	11	19.2	115.2 (6)*	96.1 (5)*
DEMSA (X.25)**	4	13.3	26.6 (2)*	26.6 (2)*
DNANS s/w** License	8	3.3-4.5	15.6 (4)*	15.6 (4)*
DNANS h/w** VAX 3100 w/disk	4	19.2	38.4 (2)*	38.4 (2)*
Total			$238.7	$207.9

** Number of units to be purchased for the specified price.*
*** E-SPAN sites at the European Space Operations Center (ESOC) FRG, European Space Research Institute (ESRIN) Italy, European Space Research and Technical Institute (ESTEC) Holland, and J-SPAN at Kyoto (Japan).*

Table 7 shows hardware and software that will be required in order to transition the backbone network to DECnet Phase V, consisting of ARC, GSFC, JPL, JSC, KSC, MSFC, plus international sites as listed.

Table 8. SPAN Site Cost to Transition to DECnet Phase V

Item	Number Needed NASA/non-NASA	GSA Cost ($ 000s)	Total Cost ($ 000s) NASA/non-NASA
DELQA* (DEQNA replacement)	150/300	0.66	99.0/198
DSV (DMV replacement)	4/30	3.4	13.6/102
DMB32 (DMR replacement)	3/40	3.5	10.5/140
DSB32 (DMR replacement)	3/40	4.9	14.7/196
Operating System** Upgrade	0/35	0.2	0/7.0
Total			$137.8/$643.0

** DEC has a trade-in policy in effect until January 1991 for DEQNA devices. The cost of a replacement DELQA with trade-in of the DEQNA is $660.*
*** Operating System upgrades are available to university sites at minimal cost (usually $100-$300 per node). The SPAN site survey has shown all systems at NASA centers currently under DEC software maintenance.*

Table 8 estimates total costs for all SPAN tail sites that will be incurred to upgrade equipment not supported under DECnet Phase V. These items include the amount necessary to replace Phase V equipment at both non-NASA SPAN tail sites and NASA sites. NASA/SPAN routing equipment has been broken out in the previous tables. The numbers were estimated from an ongoing survey of SPAN NASA and tail sites.

Table 9. Desired Equipment for SPAN Routing Centers for DECnet Phase V

Item	Number Requested	GSA Cost ($ 000s)	Potential Breakout FY91 ($ 000s)	FY92 ($ 000s)
DECmcc software*	3	0-15.75	16.0 (2)	8.3 (1)
DECmcc hardware 3100 wkstation	3	19.2	38.4 (2)	19.2 (1)
ASSET software**	3	10.0-30.0	40.0 (2)	15.0 (1)
DEC Consultant for Transitioning***	1	260.0/1yr	180.0	0
Total			$274.4	$42.5

** DECmcc software cost is based on whether the site already has the s/w licenses for the included products (Ethernim, LTM, NMCC, TSM, RBMS)*
*** ASSET software is not on GSA contract.*
**** GSA price for consultant for 10 months is $180K.*

Table 9 shows items that are not immediate requirements for DECnet Phase V, yet are highly desired and are listed in order of preference (the first 2 items must be included together). The DECmcc software reflects an average of the price, including 25-percent GSA discount. The DECmcc workstation reflects the 21-percent GSA discount.

Table 10. Proposed Distribution of DECnet Phase V Hardware and Software Components

Site	DNANS	DECmcc	Asset software
ARC	X	X	X
GSFC	X	X	X
JPL	X		
JSC	X		
KSC	X		
MSFC	X	X (FY 92)	X (FY 92)
Italy (E-SPAN)	X		
W. Germany (E-SPAN)	X		
Holland (E-SPAN)	X		
Japan	X		

Table 10 shows the proposed distribution of components purchased for use in SPAN during and after transition to Phase V.

Appendix F

Nomenclature

ADMD	Administrative Management Domain
AFI	Authority and Format Identifier
ARC	Ames Research Center
CCITT	International Telegraph and Telephone Consultative Committee
CLNP	Connectionless Network-layer Protocol
CLNS	Connectionless Network Service
CLTS	Connectionless Transport Service
CMIP	Common Management Information Protocol
CONS	Connection-Oriented Network Service
COTS	Connection-Oriented Transport Service
DCC	Data Country Code
DDN	Defense Data Network
DECmcc	Digital Equipment Corporation Monitoring and Control Center
DECnet	Digital Equipment Corporation Network
DNANS	Digital Network Architecture Naming Service
DP	Draft Proposal
DSP	Draft Standard Proposal
EDI	Electronic Data Interchange
ESA	European Space Agency
ES	End System
ESNET	Energy Science Network
ESOC	European Space Operations Center
ESRIN	European Space Research Institute
ESTEC	European Space Research and Technology Institute
FDDI	Fiber Distributed Data Interface
FIPS	Federal Information Processing Standards
FNC	Federal Networking Council
FOPG	Federal Networking Council OSI Planning Group
FRG	Federal Republic of Germany
FTAM	File Transfer, Access, and Management
FTP	File Transfer Protocol
GOSIP	Government Open Systems Interconnect Profile
GSA	General Services Administration
GSFC	Goddard Space Flight Center
HEPNET	High Energy Physics Network
IDI	Initial Domain Identifier
IDP	Initial Domain Part
IEC	International Electrotechnical Commission
IP	Internet Protocol
IS	Intermediate System
ISO	International Organization for Standardization
ISDN	Integrated Services Digital Network
ISODE	ISO Development Environment
JPL	Jet Propulsion Laboratory
JSC	Johnson Space Center
KSC	Kennedy Space Center
LTM	Local Area Network Traffic Monitor

MHS	Message Handling System
MILNET	Military Network
MSFC	Marshall Space Flight Center
NASA	National Aeronautics and Space Administration
NASNET	Numeric Aerodynamic Simulator Network
NIST	National Institute of Standards and Technology
NMCC	Network Monitoring and Control Center
NML	Network Management Listener
NSAP	Network Service Access Point
NSFNET	National Science Foundation Network
NSI	NASA Science Internet
NSIPO	NASA Science Internet Project Office
NSN	NASA Science Network
ODA	Office Document Automation
OSI	Open Systems Interconnection
OSINET	Open Systems Interconnection Network
OSPF	Open Shortest Path First
OSSA	Office of Space and Scientific Applications
PRMD	Private Management Domain
RBMS	Remote Bridge Management Software
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TCP	Transport Communications Protocol
TSM	Terminal Server Manager
VTP	Virtual Terminal Protocol
WD	Working Draft

References

[1] U.S. Government Open Systems Interconnections Profile. U.S. Federal Information Processing Standards Publication 146, Version 1, August 1988.

[2] Postel, J.B.: Internet Protocol. Request For Comment #791, Defense Data Network Information Center, SRI International. September 1981.

[3] Postel, J.B.: Transmission Control Protocol. Request For Comment #793, Defense Data Network Information Center, September 1981.

[4] ISO 7498, Basic Reference Model for Open Systems Interconnection. Information Processing Systems, 1984.

[5] ISO/IEC 8473, Protocol for Providing the Connectionless-mode Network Service and Provision of Underlying Service. Information Processing Systems, May 1987.

[6] Rose, M.T., and Case, D.E.: ISO Transport on Top of the TCP. Request For Comment #1006, Defense Data Network Information Center, SRI International, June 1987.

[7] ISO/IEC 8571-1, File Transfer, Access, and Management Part 1: General Introduction. Information Processing Systems, April 1988.

[8] Postel, J.B., and Reynolds, J.K.: File Transfer Protocol. Request For Comment #959, Defense Data Network Information Center, SRI International. October 1985.

[9] CCITT Recommendation X.400, Message Handling Systems: Systems Model-Service Elements. Red Book, 1984.

[10] Postel, J.B.: Simple Mail Transfer Protocol. Request For Comment #821, DDN Information Center, SRI International. August 1982.

[11] Virtual Terminal Service: Basic Class, Draft International Standard 9040. Information Processing Systems, August 1987.

[12] Postel, J.B., and Reynolds, J.K.: Telnet Protocol Specification. Defense Data Network Information Center, SRI International, May 1983.

[13] Rose, Marshall T.: The Open Book - A Practical Perspective on OSI. Prentice Hall, Englewoods Cliffs, New Jersey, ISBN 0-13-643016-3, 1990.

[14] Boland, Tim: Government Open Systems Interconnection Profile Users' Guide. NIST Special Publication 500-163, August 1989.

[15] Digital Network Architecture (Phase V). Digital Equipment Corporation, Maynard, Massachusetts, September 1987.

[16] ISO/IEC JTC 1/SC6/N4945: Exchange Between Systems, Intra-Domain IS-IS Routing Protocol. Telecommunications and Information, 1989.

[17] Case, J.D., Fedor, M., Schoffstall, M.L., and Davin, C.: Simple Network Management Protocol, Request For Comment #1098. Defense Data Network Information Center, SRI International, April 1989.

[18] U.S. Government Open Systems Interconnections Profile. U.S. Federal Information Processing Standards Publication 146, Draft Version 2, July 1988.

[19] Stable Implementation Agreements for Open Systems Interconnection Protocols, Version 2, Edition 4. NIST Special Publication 500-162. September 1989.

Tables

1. OSI Protocols Required for an Operational Network . . . 2
2. Product Availability for Key OSI Features 15
3. Costs of Beginning the Incorporation of OSI Products into the SPAN and NSN Backbones 28
4. Cost of Incorporating OSI Products in the Combined SPAN and NSN Backbones 32
5. Overall Cost Estimate for the SPAN Backbone, Local Site, and European Expenses 45
6. SPAN Operations Upgrade: Necessary Replacement of Obsolete, Unreliable Routing Equipment at NASA/SPAN Routing Centers . 45
7. Required Items for SPAN Backbone DECnet Phase IV to DECnet Phase V Transition 46
8. SPAN Site Cost to Transition to DECnet Phase V . . . 47
9. Desired Equipment for SPAN Routing Centers for DECnet Phase V . 48
10. Proposed Distribution of DECnet Phase Hardware and Software Components 48

Figures

1. Space Physics Analysis Network (SPAN) 7
2. NASA Science Network (NSN) 8
3. The Seven-Layer OSI Reference Model 11
4. The Lower Layers of the OSI Reference Model . . . 12
5. The Upper Layers of the OSI Reference Model . . . 13
6. Currently Defined Portions of a Complete NSAP Address or Name . 17
7. The Initial Domain Part (IDP) and the Domain Specific Part (DSP) . 36
8. Components of the IDP 36
9. Composition of the DSP Portion 37
10. GOSIP Version 2.0 OSI Architecture 41

NASA
National Aeronautics and Space Administration

Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
NASA CR-177561		

4. Title and Subtitle	5. Report Date
OSI in the NASA Science Internet – An Analysis	June 1990
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Rebecca Nitzan	A-90240
	10. Work Unit No.

9. Performing Organization Name and Address	11. Contract or Grant No.
Sterling Federal Systems, Inc. 1121 San Antonio Rd. Palo Alto, CA 94303	NAS2-11555
	13. Type of Report and Period Covered
12. Sponsoring Agency Name and Address	Contractor Report
National Aeronautics and Space Administration Washington, DC 20546-0001	14. Sponsoring Agency Code

15. Supplementary Notes

Point of Contact: Robert Carlson, Ames Research Center, MS 233-15, Moffett Field, CA 94035-1000
(415)604-6036 or FTS 464-6036

16. Abstract

The Open Systems Interconnection (OSI) protocol suite is a result of a world-wide effort to develop international standards for networking. OSI is formalized through the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The goal of OSI is to provide interoperability between network products without relying on one particular vendor, and to do so on a multinational basis.

The National Institute for Standards and Technology (NIST) has developed a Government OSI Profile (GOSIP) (ref. 1) that specifies a subset of the OSI protocols as a Federal Information Processing Standard (FIPS 146). GOSIP compatibility has been adopted as the direction for all U.S. government networks. OSI is extremely diverse, and therefore adherence to a profile will facilitate interoperability within OSI networks. All major computer vendors have indicated current or future support of GOSIP-compliant OSI protocols in their products.

The NASA Science Internet (NSI) is an operational network, serving user requirements under NASA's Office of Space Science and Applications. NSI consists of the Space Physics Analysis Network (SPAN) that uses the DECnet* protocols and the NASA Science Network (NSN) that uses TCP/IP protocols (refs. 2, 3). The NSI Project Office is currently working on an OSI integration analysis and strategy. A long-term goal is to integrate SPAN and NSN into one unified network service, using a full OSI protocol suite, which will support the OSSA user community.

*DECnet is a trademark of Digital Equipment Corporation.

17. Key Words (Suggested by Author(s))	18. Distribution Statement
Open Systems Interconnection Networking Data Communications Systems	Unclassified–Unlimited Subject Category – 62

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	59	A04

NASA FORM 1626 OCT 86

For sale by the National Technical Information Service, Springfield, Virginia 22161