FIPS PUB 179

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

GOVERNMENT NETWORK MANAGEMENT PROFILE (GNMP)

CATEGORY: HARDWARE AND SOFTWARE STANDARDS
SUBCATEGORY: COMPUTER NETWORK PROTOCOLS

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

Issued December 14, 1992

U.S. Department of Commerce
Barbara Hackman Franklin, Secretary

Technology Administration
Robert M. White, Under Secretary for Technology

National Institute of Standards
and Technology
John W. Lyons, Director

Foreword

The Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology (NIST) is the official publication relating to standards and guidelines adopted and promulgated under the provisions of Section 111(d) of the Federal Property and Administrative Services Act of 1949 as amended by the Computer Security Act of 1987, Public Law 100-235. These mandates have given the Secretary of Commerce and NIST important responsibilities for improving the utilization and management of computer and related telecommunications systems in the Federal Government. The NIST through its Computer Systems Laboratory provides leadership, technical guidance, and coordination of Government efforts in the development of standards and guidelines in these areas.

Comments concerning Federal Information Processing Standards Publications are welcomed and should be addressed to the Director, Computer Systems Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899.

James H. Burrows, Director
Computer Systems
Laboratory

Abstract

This Federal Information Processing Standard adopts the Version 1.0 GNMP. The Government Network Management Profile (GNMP) specifies the common management information exchange protocol and services, specific management functions and services, and the syntax and semantics of the management information required to support monitoring and control of the network and system components and their resources.

The GNMP builds on FIPS 146-1, Government Open Systems Interconnection Profile (GOSIP), and includes the GOSIP Version 2.0 by reference. The GOSIP specifies lower layers protocols and three applications that support general network management operations. Future versions of the GNMP will add network management functions and services for GOSIP-compliant end systems and intermediate systems. The GNMP and GOSIP are interrelated and will cross reference each other as required.

Key words: Federal Information Processing Standard (FIPS); interoperable management open systems; Government Network Management Profile (GNMP); Management Communications (CMIP/S); management information (MOs); network management; NIST OIW NMSIG; OMNIPoint 1; systems management functions.

National Institute of Standards
and Technology
FIPS PUB 179
50 pages (Dec. 14, 1992)
CODEN: FIPPAT

U.S. Government Printing Office
Washington: 1992

For sale by the National
Technical Information
Service
U.S. Department of Commerce
Springfield, VA 22161

Federal Information Processing Standards Publication 179

1992 December 14

Announcing the Standard for

GOVERNMENT NETWORK MANAGEMENT PROFILE (GNMP)

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to section 111 (d) of the Federal Property and Administrative Services Act of 1949 as amended by the Computer Security Act of 1987, Public Law 100-235.

1. **Name of Standard.** Government Network Management Profile (GNMP) (FIPS PUB 179).

2. **Category of Standard.** Hardware and Software Standards, Computer Network Protocols.

3. **Explanation.** This Federal Information Processing Standard adopts the Version 1.0 GNMP. The Government Network Management Profile (GNMP) specifies the common management information exchange protocol and services, specific management functions and services, and the syntax and semantics of the management information required to support monitoring and control of the network and system components and their resources.

The GNMP builds on FIPS 146-1, Government Open Systems Interconnection Profile (GOSIP), and includes the GOSIP Version 2.0 by reference. The GOSIP specifies lower layers protocols and three applications that support general network management operations. Future versions of the GNMP will add network management functions and services for GOSIP-compliant end systems and intermediate systems. The GNMP and GOSIP are interrelated and will cross-reference each other as required.

The primary source of specifications in the Version 1.0 GNMP is part 18 of the OIW Stable Implementation Agreements, June 1992, developed by the Open Systems Environment Implementors Workshop (OIW) sponsored by NIST and IEEE Computer Society. This source provides implementation specifications for network management based on the service and protocol standards issued by the International Organization for Standardization (ISO).

4. **Approving Authority.** Secretary of Commerce.

5. **Maintenance Agency.** U. S. Department of Commerce, National Institute of Standards and Technology, Computer Systems Laboratory.

6. **Cross Index.**

a. NIST Special Publication 500-202, Stable Implementation Agreements for Open Systems Interconnection Protocols, Version 5, Edition 1, NIST Workshop for Implementors of Open Systems Environment, June 1992.

b. FIPS PUB 146-1, Government Open Systems Interconnection Profile (GOSIP).

7. **Related Documents.** Related documents are listed in the Reference Section of the GNMP document.

8. **Objectives.** The primary objectives of this standard are:

- to achieve interconnection and interoperability of computers and systems that are acquired from different manufacturers in an open systems environment;
- to reduce the costs of computer network systems by increasing alternative sources of supply;
- to facilitate the use of advanced technology by the Federal Government;
- to stimulate the development of commercial products compatible with Open Systems Interconnection (OSI) standards.

9. Specifications. GNMP (affixed)

10. **Applicability.** GNMP shall be used by Federal Government agencies when acquiring network management functions and services for computer and communications systems and networks.

11. **Implementation.** This standard is effective June 14, 1993. Until December 14, 1994, agencies are permitted to acquire alternative network management functions and services which provide equivalent functionality to this standard. Agencies are encouraged to use this standard for solicitations and contracts for new network management functions and services to be acquired after June 14, 1993. This standard is compulsory and binding for use in all solicitations and contracts for new network management functions and services to be acquired after December 14, 1994. Additional management support functions will be added to GNMP as implementation specifications for these functions are developed by the Workshop for Implementors of Open Systems Environment. For a period of 18 months after these new functions are included in GNMP, agencies are permitted to acquire alternative functions and services which provide equivalent functionality. After the 18-month period, the new functions and services should be cited in solicitations and contracts when systems to be acquired provide equivalent functionality to the protocols defined in the GNMP document.

12. **Waivers.** Under certain exceptional circumstances, the heads of Federal departments and agencies may approve waivers to Federal Information Processing Standards (FIPS). The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of Title 44, U.S. Code. Waivers shall be granted only when:

a. Compliance with a standard would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or
b. Cause a major adverse financial impact on the operator which is not offset by Governmentwide savings.

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

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

When the determination on a waiver applies to the procurement of equipment and/or services, a notice of the waiver determination must be published in the *Commerce Business Daily* as a part of the notice of solicitation for offers of an acquisition or, if the waiver determination is made after that notice is published, by amendment to such notice.

A copy of the waiver request, any supporting documents, the document approving the waiver and any supporting and accompanying documents, with such deletions as the agency is authorized and decides to make under 5 U.S.C. Sec. 552(b), shall be part of the procurement documentation and retained by the agency.

13. **Special Information.** The GNMP is being developed in phases. Version 1.0 GNMP specifies the initial phase of the GNMP. Additional management capabilities and managed objects will be included in subsequent releases of the profile. Eventually, as the NM standards all reach technical maturity, the GNMP will embrace the full set of management functionality.

14. **Where to Obtain Copies.** Copies of this publication are for sale by the National Technical Information Service (NTIS), U.S. Department of Commerce, Springfield, VA 22161. When ordering, refer to Federal Information Processing Standards Publication 179 (FIPSPUB179), and title. Specify microfiche if desired. Payment may be made by check, money order, or NTIS deposit account.

Federal Information
Processing Standards Publication 179
1992 December 14

Specifications for

GOVERNMENT NETWORK MANAGEMENT PROFILE (GNMP)

Government Network Management Profile
(GNMP)

Contents

List of Figures

Preface

This is Version 1 of the Government Network Management Profile (GNMP). Section 1 contains introductory material, the purpose and scope of the profile, and the sources of the specifications contained in the profile. Section 2 describes how to use this profile. Section 3 provides a brief tutorial overview of the OSI management standards included in this profile. Section 4 specifies conformance requirements to this network management profile, while Section 5 contains testing requirements for GNMP-compliant implementations.

This profile will change with improvements in technology and with the evolution of network management standards. Appendix A specifies future work items planned for subsequent versions. Appendix B provides information on where GNMP-related documents can be obtained. Appendix C provides definitions for the acronyms used in this document. Appendix D contains a glossary of the terms frequently used in this document.

1. Introduction

To provide background information on network management (NM), this section discusses the urgent need for integrated NM tools and examines the status of NM standards and of Implementation Agreements (IAs). Next, the purpose and scope of the GNMP and its applicability to federal government procurement are described. Lastly, the approach taken for the development of the GNMP is presented, the sources of specifications are listed, and the relationship of the GNMP to the Government Open Systems Interconnection Profile (GOSIP) and to the Industry/Government Open Systems Specification (IGOSS) is explained.

1.1. Need for Integrated Tools on Network Management

Network management is **vital to the practical operation of large networks.** Usage of network services is affected by the availability and effectiveness of network management capabilities. Presently, network control and monitoring activities, when available, are accomplished primarily through the use of proprietary tools and/or software in a piecemeal, non-integrated manner. Network operations managers categorize their problems in one of two ways. In one situation, NM tools come from different vendors and function in proprietary methods; however, these tools do not interoperate in an integrated manner. This increases cost and inefficiency in managing networks. In the other situation, NM tools come from a single vendor and, consequently, operate in an integrated manner. Thus, the network owner, in order to obtain this integration, may not be able to procure management products from other vendors, even when such products might be less costly or more desirable technically. The need for products to manage components of multi-vendor networks in an integrated manner is quite real, well-documented, and urgent; and the need is increasing. The U.S. Government, with its multiplicity of computer systems and communications networks, requires integrated NM tools from multiple vendors.

1.2. Status of OSI Network Management Standards, Implementors Agreements, and Specifications

The Open Systems Interconnection (OSI) management standards are maturing rapidly. These are being developed collaboratively by the International Organization for Standardization-/International Electrotechnical Committee (ISO/IEC) and the International Telegraph and Telephone Consultative Committee (CCITT) in the X.700 series of documents. The ultimate goal of these standards is to enable the development of interoperable, multi-vendor products for the management of computer and communications systems and networks. Key areas of management standardization are architecture, protocols, systems management functions, and the structure of management information. The Common Management Information Services and Protocol (CMIS/P) standards [CMIS] [CMIP] and some systems management functions are now International Standards (ISs). Many other needed management standards are still either being planned and proposed, or are at the Draft International Standard (DIS) status. However, those ISs currently available comprise a subset of management standards that make it possible for

vendors to build useful systems to meet some immediate network management requirements. This set of standards is included in GNMP. Those standards that are being developed by the CCITT and ISO/IEC, such as the Software Management Function and the Time Management Function, as they mature, will be considered for inclusion in later versions of this profile.

Another important aspect of network management standards activity is the development of Implementation Agreements (IAs). The Network Management Special Interest Group (NMSIG) of the Open Systems Environment (OSE) Implementors' Workshop (OIW) (sponsored by NIST and the IEEE Computer Society) is developing IAs based on the emerging NM standards. These agreements are being developed in phases that align with the ISO/IEC standards as they progress from DIS to IS. Version 1 GNMP is based on the June 1992 stable IAs [STABLE].

An international partnership of government and industry, vendors and users, the Open Management Roadmap, initiated and managed by the Network Management Forum (NMF), is an endeavor to coordinate all the related network management activities of developing standards and defining specifications to produce interoperable network management products. Currently, the partnership includes: Her Majesty's Treasury, U.K. (CCTA), European Community Testing Service for Network Management (CTS3/NM), National Institute of Standards and Technology (NIST), Network Management Forum (NMF), X/OPEN, Object Management Group (OMG), the Open Software Foundation (OSF), Corporation for Open Systems (COS), Interoperability Technology Association for Information Processing (INTAP), Standards Promotion and Application Group (SPAG), UI (UNIX International), and the User Advisory Council (UAC). Standards organizations and regional workshops, such as the OIW, are source organizations in the Roadmap activity. The Roadmap defines a number of Open Management Interoperability Points (OMNI*Points*) which are snapshots of standards, specifications, and agreements for NM to which the vendor partners agree to develop products and for which the user partners expect to purchase products. The first OMNI*Point* specification, OMNI*Point* 1, is scheduled for release in August, 1992. Version 1 GNMP will be an integral part of OMNI*Point* 1.

Recently the U.S. DOD has proposed a military standard for network management. The standard is an output of the Defense Computer Protocol Standards (DCPS) Technical Management Panel (DTMP) working group on network management. Called the Network Management Specification for DOD Communications (MIL-STD-2045-38000), this specification builds on Version 1 GNMP and augments GNMP with military unique requirements for network management. Version 1 GNMP and the military standard are companion documents to be taken in concert when specifying military needs for network management.

1.3. Purpose

Within the government, systems and network management can best be accomplished by using a single profile to specify all the standards to which NM products must comply. In the absence, at present, of a complete set of mature standards for NM, a set of initial NM specifications that contains a useful subset of the planned systems and network management functionality provides

an interim solution to meet some high priority requirements. NIST is, therefore, promulgating this Federal Information Processing Standard (FIPS) for network management.

1.4. Scope

The GNMP is scoped in terms of OSI systems management. Version 1 GNMP specifies a common management information exchange protocol and services, systems management functions and services, and the syntax and semantics of the management information required to support monitoring and control of network and system components and their resources.

In particular, Version 1 GNMP specifies: 1) the Common Management Information Services and Protocol (CMIS/P); 2) management information definitions (referenced in section 4 of the GNMP); 3) the following seven systems management functions (SMFs):

- Object Management Function,
- State Management Function,
- Attributes for Representing Relationships,
- Alarm Reporting Function,
- Event Report Management Function,
- Log Control Function,
- Security Alarm Reporting Function;

and 4) for security, two optional peer entity authentication modes.

1.5. Applicability

The GNMP is the standard reference for all Federal Government agencies to use when acquiring Network Management (NM) functions and services for computer and communication systems and networks.

1.6. Approach

The GNMP is being developed in phases resulting in several planned versions of the document. This is the initial version of the GNMP. Additional management capabilities and managed objects will be included in subsequent releases of the profile. Eventually, as the NM standards all reach technical maturity, the GNMP will embrace the full set of management functionality

For the development of the initial version, a three-step approach was taken:

(1) analysis of NM requirements,
(2) comparison of requirements with emerging standards and implementors' agreements, and
(3) proposals to resolve any essential, unmet needs/requirements.

The purpose of the requirements analysis was to assure that the GNMP addresses real needs. Network management requirements were collected from a survey, conducted by NIST in the summer of 1990, of federal agencies. Survey results indicated that management of local area networks (LANs), as well as the bridges that interconnect them, represents a key requirement. Furthermore, access control to NM information was considered to have the highest priority among all the network management security requirements.

The NM requirements identified from the survey were compared with the emerging NM standards and IAs. An obvious need recognized by the comparison study was the requirement for management information definitions. Although some support management information (MI) has been defined by the International Organization for Standardization/International Electrotechnical Committee (ISO/IEC) NM working group and although they have specified a set of guidelines and templates for defining MI, the working group has not specified the definitions of particular MI to be monitored and controlled. Using the standard definition templates that ISO/IEC has developed, various standards-making groups and implementors forums are currently developing definitions of MI pertinent to their specific areas of expertise and standardization.

In the GNMP, management information has been divided into three categories corresponding to the three planned versions of the GNMP. The focus of each version has been determined in accordance with the prioritized NM requirements obtained from the survey. Version 1 GNMP focuses on definitions of management information pertaining to implementations that perform layer 1 and 2 functions of the OSI reference model [BRM]. Management information for layer 3 and 4 functionalities are also included since they are international standards and are highly needed by the users as the survey indicated.

Defining management information not only requires in-depth knowledge of the specific subject areas to which the management information belongs, but also requires understanding of the management information model and the standard templates. Consequently, it takes extended development time to define specific management information. For various LAN technologies, Version 1 GNMP includes those MI definitions that have reached international or national standard status. Additional MI definitions for layer 1 and 2 functions are expected to be included in later versions of GNMP as they reach stable standard status.

1.7. Sources of Specifications

The primary source of specifications in the Version 1 GNMP is part 18 of the OIW Stable Implementation Agreements (SIAs), June 1992 [STABLE]. This source provides implementation specifications for network management based on the service and protocol standards issued by the ISO/IEC.

Since the OIW IAs continue to evolve and the NM IAs are still incomplete, additional sources of specifications are included in Version 1 GNMP in order to meet the minimum requirements of Version 1 GNMP. Additional sources of specifications for Version 1 GNMP include those standards committees and vendors/users consortia which have developed definitions of needed management information:

- IEEE 802.1B Local and Metropolitan Area Networks Management [L/MAN],
- IEEE 802.3 Repeater management [HUB],
- ANSI X3T9.5 FDDI Station Management [FDDI],
- CCITT Study Group IV Generic Network Information Model [CCITT], and
- ISO/IEC JTC1/SC6 Transport and Network Layer Management [ISIS], [NW], [XPORT].
- Network Management Forum [NMFMIL].

1.8. GNMP and GOSIP

GNMP and GOSIP Version 2 are both government procurement specifications of open systems. GOSIP is cited in the GNMP to specify the protocol stack upon which management information can be conveyed. GOSIP also specifies services, such as File Transfer, Access and Management (FTAM), Message Handling System (MHS),and Virtual Terminal (VT), that can be used to support network management applications. Version 3 GOSIP will cite the GNMP to specify the management protocols, services, and information needed to facilitate interoperable multi-vendor management of GOSIP-compliant systems. As both GNMP and GOSIP mature, it is expected that they will continue to cross-reference the latest versions of each other.

1.9. GNMP, GOSIP, and IGOSS

The Industry/Government Open Systems Specification (IGOSS) is an OSI procurement specification that the federal government plans to issue jointly with the Manufacturing Automation Protocol (MAP), the Technical and Office Protocols (TOP), and the Electric Power Industry's Unified Communications Architecture (UCA). Version 3 of GOSIP will primarily be a reference to IGOSS. The GOSIP will also include a statement of applicability for federal agency users and will include any protocols required by the federal government but not jointly agreed by the IGOSS participating organizations. All material relating to network management will be contained in the IGOSS either directly or by reference to the GNMP.

1.10. GNMP and OMNI*Point* 1

The development of the GNMP was the impetus for the Network Management Forum to initiate the Open Management Roadmap activity. From the outset of that activity, NIST has been a partner in this international partnership of government and industry groups who were interested in interoperable network management. The Roadmap partnership agreed to a plan for defining a number of Open Management Interoperability Points (OMNI*Points*) which are snapshots of standards, specifications, and agreements for network management. As a result of NIST participation, the OMNI*Point* 1 specifications will include the GNMP as an example procurement document whose requirements may be met by OMNI*Point* 1 products. Continued collaboration and participation in the Open Management Roadmap is expected as the GNMP evolves and additional OMNI*Points* are defined.

2. How to Understand and Use the GNMP

Businesses and governments continue deployment of voice and data communication networks at an increasing pace. The deployment of these networking devices is generating intense pressure for suppliers to provide network management products as well. Suppliers are responding with capable, but incompatible, network managers. The result in most large organizations today is a loose confederation of multi-vendor systems managed by a variety of network management products. The situation in a typical company is illustrated in Figure 2.1. In the example, five different terminals are required to manage all the network assets, and nowhere is an integrated view available.

The solution to this dilemma depends upon an integrated network management system. For the company illustrated in Figure 2.1, a solution such as that shown in Figure 2.2 might be feasible. All five network managers (the two LAN managers, the wide-area network (WAN) manager, the telecommunications manager, and the PBX manager) remain in place, using proprietary means to manage specific resources. Four network management integrators have been added: one integrates the LAN managers, one integrates the telecommunications managers, one integrates the WAN manager and the LAN integrator, and one integrates the telecommunications and data communications integrators. Implementation of such a hierarchical network management system requires a standard for network management information exchange between integrators, and between integrators and managers. In Figure 2.2, interfaces requiring such a standard are shown with broken lines connecting the label "GNMP."

The Government Network Management Profile (GNMP) specifies a standard for the exchange of management information between integrators and between integrators and managers. The GNMP specification can also be used between managers and network elements, should the network elements possess sufficient computing capability. The scope of the GNMP encompasses a set of protocols for multi-vendor communications, a set of general-purpose management functions, and a standard set of managed object definitions. This scope addresses only the exchange of management information in a standard way in order to achieve integration of management systems and components made independently by a variety of suppliers.

Other important issues are outside the scope of the GNMP. Consider, for example, the analysis of management information. For any operational network management system, raw management data must be collected, stored, calculated, and correlated to provide useful outputs for network planning, fault prediction, and billing. Requirements in these areas are outside the scope of the GNMP and must continue to be specified directly by the Acquisition Authority. Human-machine Interface (HMI) is also outside the scope of the GNMP. The Acquisition Authority must continue to specify any requirements regarding presentation and ease of use. The usual issues of configuration and sizing of network management components are also outside the scope of the GNMP. The Acquisition Authority must continue to plan the deployment and sizing of specific integrators and managers in accordance with operational requirements. The GNMP, then, addresses a single, significant network management integration problem: interoperability between network management components.

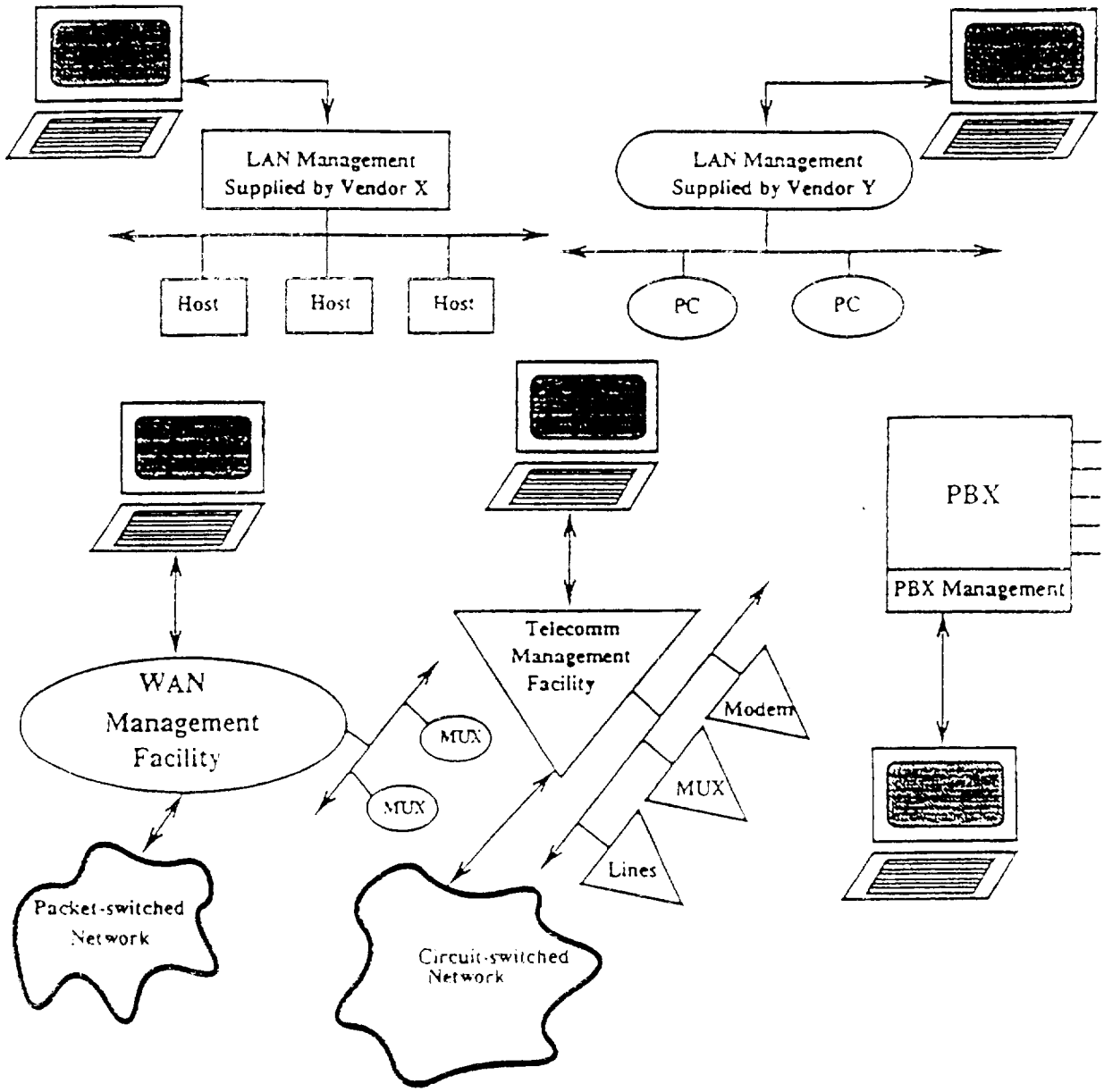


Figure 2.1 Network Mangement in a Non-integrated Manner

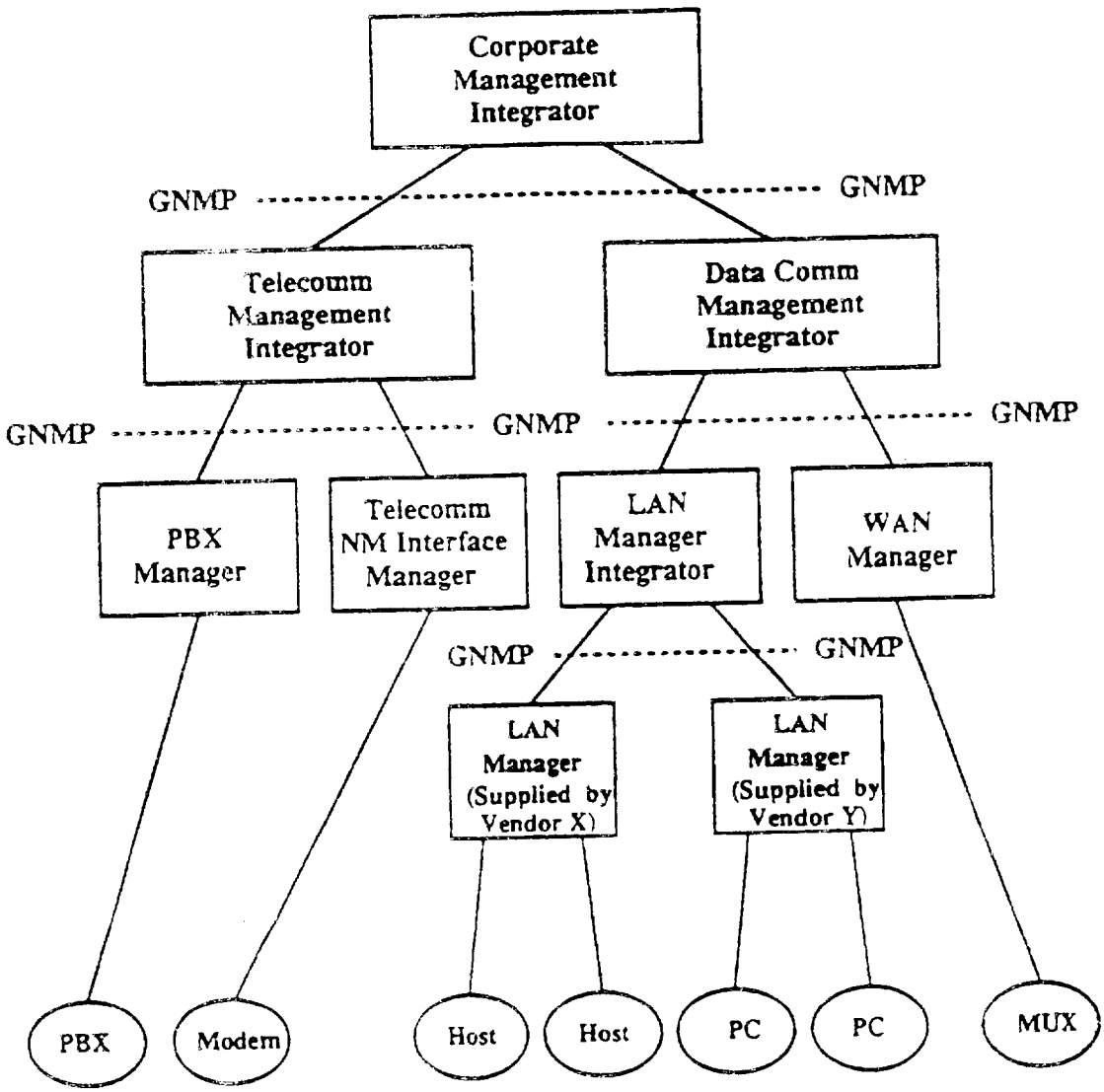


Figure 2.2 Integrated Network Management Using GNMP

Version 1 GNMP includes the international standard Common Management Information Protocol (CMIP) and seven general management support functions. More management support functions will be included in future versions as these functions become available. Version 1 GNMP incorporates managed object definitions for network interfaces, including both data and voice communication network components. Additional managed objects are planned in future versions as stated in Appendix A.1. The eventual scope of the GNMP will be extended to include system management objects for applications, services, operating systems, and database systems. Version 1 GNMP includes optional methods of authentication. These optional authentication methods are provided for interim use in the absence of standard approaches to network management security. Regarding access control, the GNMP assumes that a properly authenticated user should have access to any management information available. Future versions of the GNMP will provide finer-grained access control as appropriate standards are agreed.

The GNMP builds on the Government Open Systems Interconnection Profile (GOSIP). In fact, the GNMP includes the GOSIP Version 2, by reference. The GOSIP specifies protocol layers 1 through 6 to provide basic interoperability in support of CMIP. In addition, the GOSIP Version 2 provides three applications that might be useful in a general purpose network management solution. The File Transfer, Access, and Management (FTAM) application facilitates the transfer of bulk information, such as routing tables, billing records, audit trails, and configuration data. The Virtual Terminal (VT) application enables remote login to network management systems, thus, allowing a network operator to execute proprietary network management tools and diagnostics. The Message Handling System (MHS) permits network operators to exchange messages with each other while attempting to diagnose or correct network problems. MHS can also be employed to alert users about network status changes. Future versions of the GNMP will include additional managed object definitions for layers three through seven for GOSIP-compliant end systems and for layer three for GOSIP-compliant intermediate systems. Thus, the GNMP and the GOSIP are tied intimately, cross-referencing each other as required.

With the foregoing background information, an Acquisition Authority can understand how to use the GNMP to specify interoperable network management interfaces for components in a network management system. First, the Acquisition Authority must develop a plan for partitioning network management responsibilities among network managers and for interconnecting the managers through network integrators. The specific number, location, scope, and size of the managers and integrators will depend on the operational requirements of the Acquisition Authority. Second, the Acquisition Authority must decide whether or not authentication is required, and if so, which specific option is needed. Third, the Acquisition Authority must determine which optional GOSIP applications, if any, are required for each manager and integrator. Fourth, the Acquisition Authority must select the managed objects required to be supported for each manager and integrator. For each selected managed object, the Acquisition Authority must determine if any of the optional attributes and conditional packages are required to be supported. For the selected managed objects, the Acquisition Authority must decide the name bindings which define the relationships between instances of managed objects needed to

support the operational requirements. Having made these decisions, the Acquisition Authority can use the GNMP to specify protocol requirements for each manager and integrator, so that interchange of management information can be achieved. NIST is developing a Users' Guide to Version 1 GNMP. This guide will address the issues related to preparation of a Request for Proposal (RFP) for network management. Beyond the GNMP, the Acquisition Authority must specify Human-machine Interface requirements, management data analysis requirements, system and component capacity and performance requirements, and any other requirements.

In summary, the GNMP is a useful tool to specify interfaces between managers and integrators to enable exchange of management data and execution of management functions when the managers and integrators might be provided by a variety of suppliers. The GNMP permits significant flexibility regarding many engineering issues, and can be tailored to some degree for specific requirements. This initial version of the GNMP is simply a beginning; future enhancements, as outlined in Appendix A, are already foreseen.

3. Description of Network Management Standards

This section provides an overview of the OSI management standards. First, the organization and interrelationships of these standards are explained; then each standard is briefly described. The information in this section is intended to be tutorial. The standards included in this profile are specified in section 4, GNMP conformance requirements.

The international standards for the management of networks are rapidly approaching maturity. These standards jointly provide a foundation for the development of interoperable NM products. The primary goal for developing interoperable NM products is to allow network managers to remotely monitor and control network resources residing on network components developed by different vendors. In order to accomplish this, there must be a common method for transferring the management commands and management information; and there must be a common view of management information. To exchange management commands and information, OSI management defines a standard management protocol, known as the Common Management Information Protocol (CMIP). To provide a standard representation of management information, a set of standards, called the Structure of Management Information (SMI), has been developed. In addition to CMIP and SMI, a set of standards, known as the Systems Management Functions (SMFs), is also being developed to define specific services and protocols to support network management. These services satisfy the requirements of the Specific Management Functional Areas (SMFA) [FRMWK] including configuration, fault, security, performance, and accounting management.

As specified in the Systems Management Overview (SMO) [SMO], OSI management standards are subdivided into four groups:

(1) *Standards specifying the architecture and organization of OSI Management* - This group of standards includes the Management Framework [FRMWK] and the Systems Management Overview [SMO]. Presently, the Management Framework and the Systems Management Overview are both international standards (ISs).

(2) *Standards for the communication of management information* - This group of standards includes the Common Management Information Services (CMIS) [CMIS] and the Common Management Information Protocol (CMIP) [CMIP]. These two standards specify how the exchange of management information between two open systems is accomplished. CMIS and CMIP are ISs. Subsection 3.1 describes the CMIS and CMIP standards.

(3) *Standards relating to the structure of management information (SMI)* - The standards in this group specify the syntax of information which is transferred for management purposes. The standards that support the specification of management information are: the Management Information Model [MIM], the Definition of Management Information [DMI], and Guidelines for the Definition

of Managed Objects [GDMO]. These standards have reached IS status. Subsection 3.2 briefly describes each of these standards. Additionally, there are two emerging standards related to management information. They are Generic Management Information (GMI) [GMI] and Requirements and Guidelines for Implementation Conformance Statement Proformas Associated with Management Information (MOCS) [MOCS]. These standards are Draft International Standards (DISs).

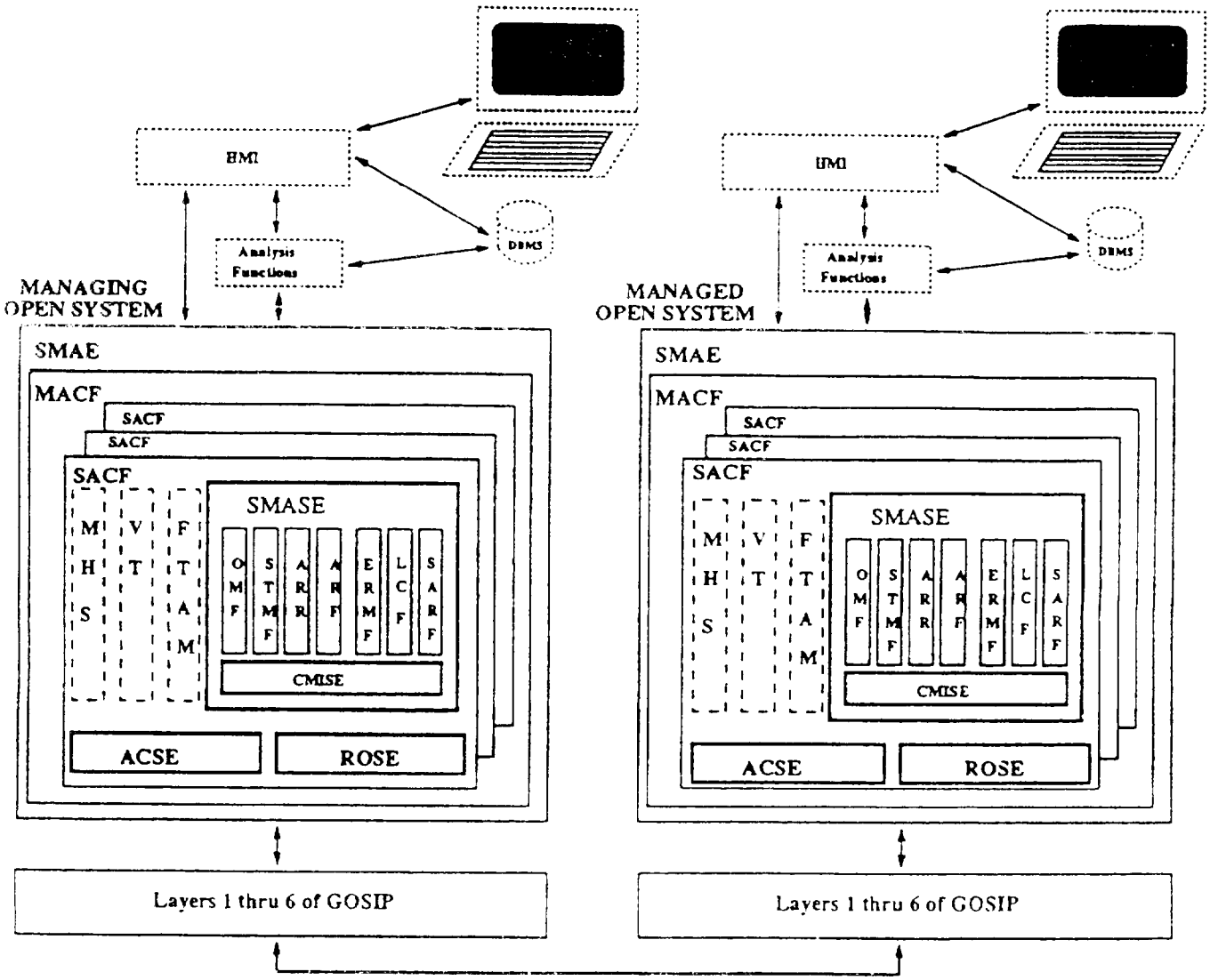
(4) *Standards for systems management functions (SMFs)* - The standards in this group define the services and, if appropriate, the functional units and generic definitions of managed objects required for each specific systems management function. The SMF standards are at various stages of development, ranging from working proposals to CDs, DISs and ISs. The Object Management Function [OMF], the State Management Function [STMF], Attributes for Representing Relationships [ARR], the Alarm Reporting Function [ARF], the Event Report Management Function [ERMF], the Log Control Function [LCF] and the Security Alarm Reporting Functions [SARF] are ISs. Other SMFs (such as the Workload Monitoring Function, the Summarization Function, and Objects and Attributes for Access Control) are at various stages of development as international standards. Subsection 3.3 describes the seven SMFs included in Version 1 GNMP.

Standards related to network management security are currently being developed by various standards groups. Section 3.4 describes the security options included in Version 1 GNMP.

Taken together, these NM standards define aspects of NM that must be implemented in a standard way to allow interoperable, multi-vendor management. Figure 3.1 illustrates how these management standards fit in the application layer structure in an open system. For a detailed description of the architecture of the application layer, see the international standard, Application Layer Structure [ALS]. Those non-standardized, but generally required, NM elements, such as human-machine interface, are also included in the illustration and are designated as recommended elements. Application layer standards, such as FTAM, that may be used by network management applications are included in the figure as well; these are designated as optional elements.

3.1. Management Communications

Network management requires the ability to communicate management information and commands between open systems. The management communication protocol and service provide an information transfer mechanism, mutually agreed by peer participating management entities. The service and protocol developed by ISO/IEC for OSI systems management are the Common Management Information Service (CMIS) and the Common Management Information Protocol (CMIP). CMIP is the application layer protocol used in the OSI environment to transfer management commands and information between open systems. CMIP specifies the



ARF: Alarm Reporting Function
ACSE: Association Control Service Element
ARR: Attributes for Representing Relationships
CMISE: Common Management Information Service Element
DBMS: Database Management System
ERMF: Event Reporting Management Function
FTAM: File Transfer, Access and Management
GOSIP: Government OSI Profile
LCF: Log Control Function
MACF: Multiple Association Control Function
MHS: Message Handling System
HMI: Human Machine Interface
OMF: Object Management Function
ROSE: Remote Operations Service Element
SACF: Single Association Control Function
SARF: Security Alarm Reporting Function
SMAE: Systems Management Application Entity
SMASE: Systems Management Application Service Element
STMF: State Management Function
VT: Virtual Terminal

LEGEND

Recommended but not standardized

Optional

Figure 3.1 Components of Interoperable Management Open Systems

makeup of the management messages, while CMIS specifies the service interface to management information service users. Although not stated in these particular standards, normally in any example of management communication, the management entity on one end of the association assumes a manager role, while the peer management entity on the other end of the association assumes the agent role.

3.1.1. Common Management Information Protocol (CMIP)

CMIP provides a commonly understood format for the transfer of management information and commands between the peer management entities. Typically, one of the peers acts in a manager role and one acts in an agent role during management communications. CMIP specifies the generic transfer mechanism needed by the systems management functions (e.g., OMF, STMF). The types of management information and commands that are exchanged using CMIP take the general form of event notifications, information or action requests, and responses, containing either the requested information or some indication as to why the request failed.

3.1.2. Common Management Information Services (CMIS)

CMIS provides a full range of services by means of a small number of basic service primitives. The major ones are: 1) M-GET, a read operation to retrieve attribute values of managed objects; 2) M-SET, a write operation to permit the setting of managed object attribute values; 3) M-EVENT-REPORT, an operation to transmit relevant information concerning significant predefined occurrences on one system (e.g., an agent) which are to be reported to another system (e.g., its manager); and 4) M-ACTION, an operation intended to remotely invoke a predefined management activity on a managed object located on the target system. The ability to establish new management information object instances, or to remove no longer needed management information object instances, is supported by the CMIS service primitives, M-CREATE and M-DELETE, respectively. The M-CANCEL-GET service primitive allows cancellation of a previously requested and currently outstanding invocation of the M-GET service.

The intent of the CMIS service primitives is to allow the management service user: 1) to specify the management operation (command) being transmitted; 2) to pass appropriate support information; 3) to pass result or error information; 4) to identify the particular managed object/attribute/action/event to be operated upon, either by directly naming the specific object instance or by specifying criteria by which an appropriate set of objects can be selected (i.e., through the use of "scoping," to select potential object targets, and "filtering," to select the actual targets which satisfy a specified set of conditions); 5) to identify the particular instance of management communication; 6) to pass access control information; and 7) to specify when operations and events occurred.

CMIS capabilities are partitioned into functional units which can be negotiated between peer management applications communicating over a given association. The resulting negotiated agreement limits the range of management communication allowed on that association. The kernel functional unit of CMIS includes all the basic service primitives mentioned above. This kernel functionality can be augmented by negotiating functional units which make available services within CMIS multiple object selection (scoping), multiple reply and filtering in order to select sets of objects to be operated on and to allow multiple replies in such cases. An additional functional unit makes available the extended use of presentation layer services.

3.2. Management Information

To provide interoperability among network management systems, each system must have a common "view" of management information. This involves first assuring that the abstract conceptual view of management information is consistent. Within this consistent management information model, then, management information must be defined in a consistent way. Finally, a registration methodology and a repository for management information definitions are required, so that general access is provided to these definitions.

Several international standards exist to facilitate a common view of management information. These standards provide: 1) an overview and model of management information, 2) a generic approach to and format for defining management information, and 3) certain specific definitions of managed objects to support network management functions. The following three subsections expand upon each of these documents. The fourth subsection to follow discusses issues related to the actual definitions of management information (managed objects).

3.2.1. Management Information Model (MIM)

The Management Information Model [MIM] describes an object-oriented model of management information. This model divides management information into managed objects, their attributes, the management operations that can be performed upon them, and the notifications that they can emit. The set of managed objects in an open system, together with their attributes, constitute that open system's management information base. Using object-oriented principles, the management information model defines key concepts such as inheritance, allomorphism, containment and naming, as they relate to managed objects.

3.2.2. Guidelines for the Definition of Managed Objects (GDMO)

The Guidelines for the Definition of Managed Objects [GDMO] specifies how management information definitions shall be defined, what notational tools are to be used in such definitions, and what documentation structure is to be used for managed object class definitions. Included in GDMO are templates for management information definitions. These templates provide

common, detailed descriptions for defining managed object classes, name bindings, attributes, actions and notifications.

3.2.3. Definition of Management Information (DMI)

The Definition of Management Information [DMI] defines often used managed object classes, packages, attribute types, specific attributes, action types, parameter types, and notification types. DMI also specifies compliance requirements placed on other standards that make use of the definitions.

DMI provides generic definitions that support systems management functions and can thus be incorporated in other management information definitions. These definitions may also be used in other standards to specify objects, attributes, notifications and action types.

3.2.4. Management Information Definitions

The GNMP includes the OIW Management Information Library (MIL). The OIW MIL contains management information definitions which were aligned with that of the Network Management Forum (NMF). Recall that the focus of Version 1 GNMP is on layers 1 and 2. Unfortunately, the managed objects in the OIW MIL are insufficient to enable management of LANs and other devices which provide layer 1 and 2 functionality. Additional management information definitions are required. In order to augment the OIW MIL definitions and to provide the necessary managed object definitions to support management of layer 1 and 2 functionality, additional managed object definitions are included in Version 1 GNMP. These additional definitions include management information being developed by IEEE 802 (for LANs and Repeaters), ANSI X3T9.5 (for FDDI), CCITT SG IV (for telecommunication networks), ISO/IEC Joint Technical Committee 1 (JTC1) / Subcommittee 6 (SC6) (for Transport and Network Layer protocols), and Network Management Forum.

3.3. Systems Management Functions

To develop functions for the support of systems management, ISO/IEC has partitioned systems management activities into five Specific Management Functional Areas (SMFAs): configuration management, fault management, performance management, security management, and accounting management. Within each of these SMFAs, ISO/IEC groups are developing standards for functions (including requirements, models, and services) for the management of networks. Because of overlap among requirements of the SMFAs, management functions developed to satisfy the needs of one SMFA can often be used in support of other SMFAs. The functions developed by the SMFA groups of ISO/IEC are known as Systems Management Functions (SMFs). Seven of these SMFs are included in Version 1 GNMP: Object Management Function (OMF), State Management Function (STMF), Attributes for Representing Relationships

(ARR), Alarm Reporting Function (ARF), Event Report Management Function (ERMF), Log Control Function (LCF), and Security Alarm Reporting Function (SARF). The following SMFs are under development by ISO/IEC, but are not included in this version of GNMP: Security Audit Trail Function, Objects and Attributes for Access Control, Accounting Metering Function, Workload Monitoring Function, Test Management Function, Changeover Function, General Relationship Model Function, Management Domain Function, Management Knowledge Management Function, Response Time Monitoring Function, Scheduling Function, Time Management Function, and Summarization Function. The intention of the standards community is to develop additional SMFs as needs are identified. As additional SMFs reach maturity and become standardized, they will be considered for inclusion in future versions of the GNMP. Brief summaries of each of the seven SMFs included in Version 1 GNMP are presented in the subsections that follow.

3.3.1. Object Management Function (OMF)

Managed objects provide a view of system resources that may be managed using OSI management protocols. The OMF enables a management user to create, delete, examine or modify characteristics of managed objects. The OMF describes the following services: reporting of the creation and deletion of managed objects and reporting of changes of attribute values of managed objects. The OMF also describes, so called, "pass-through" services which map directly to CMIS. These include: creating and deleting managed objects, performing actions upon managed objects, changing attribute values, reading attribute values, and reporting events. For details on each of these services see the Object Management Function Standard [OMF].

3.3.2. State Management Function (STMF)

The State Management Function defines three attributes whose values are used to indicate or control the state of a resource represented by a managed object. These attributes are: operational state, usage state, and administrative state. The value of the operational state attribute indicates whether or not the resource is physically installed and/or working. The value of the usage state attribute indicates whether the resource is active, and if it is, whether the resource has spare capacity for additional users. The value of the administration state attribute indicates whether the use of a resource is permitted or prohibited. The value of the administrative state may be set through the use of management services. The STMF defines generic attributes and operations that can be part of any managed object definition in order to provide a standardized OSI management technique for dealing with management states. The STMF provides the management user the ability to examine states, to be notified of changes in state, to monitor overall operability and usage of resources in a consistent manner, and to control the general availability of specific resources. For details on the factors affecting the states of a managed object and the set of attributes and notifications (described in section 3.3.5) related to state management see the standard [STMF].

3.3.3. Attributes for Representing Relationships (ARR)

According to the Attributes for Representing Relationships (ARR) standard [ARR], managed objects may be related in one of the following three categories of relationships: containment relationships, reciprocal relationships, and one-way relationships. Containment relationships are defined in the Management Information Model (MIM) standard [MIM]. Reciprocal and one-way relationships are defined in ARR. The ARR standard provides a model for specifying relationships among managed objects and indicates which attributes, defined in the Definition of Management Information (DMI) standard [DMI], are to be included in managed object definitions for the purpose of representing these relationships. Relationships are used to provide a set of rules governing how one part of an open system may affect other parts of the system.

In addition to describing the nature and types of managed object relationships and how they are represented, ARR describes the monitoring and controlling of these relationships. Beyond the basic management capabilities of reading and setting attribute values which represent these relationships, ARR defines a service which specifies how notifications (described in section 3.3.5) of relationship changes are to be reported. A description of the different types of relationships and the generic relationship attributes is provided in the ARR standard.

3.3.4. Alarm Reporting Function (ARF)

The ARF specifies particular categories of alarms as well as a mechanism for communicating these alarms between peer management users. The ARF [ARF] specifies the following five basic categories of alarms along with their parameters and semantics: communications, quality of service, processing failure, equipment, and environmental. Included within the description of these alarm types are parameters and semantics. Some examples of alarm causes are queue size exceeded, retransmission rate excessive, and out of memory.

The alarms discussed in the ARF are particular types of notifications (described in section 3.3.5) which convey information about detected faults and abnormal conditions. The ARF, therefore, supports the network management capability of detecting faults, or those abnormal conditions generally leading to faults, as early as possible, and preferably before problems are noticed by the network users. For details on each of these categories of alarms see the ARF standard.

3.3.5. Event Report Management Function (ERMF)

Management events indicate that some measurable activity has occurred in a network management system. When an event has occurred within a managed object, a notification is emitted by the object. Notifications are passed through discriminators, which specify conditions that must be satisfied prior to generating an event report. The ERMF standard [ERMF] discusses discriminators and provides the management user the following capabilities: the definition of a flexible event report control service, the specification of destinations to which

event reports are to be sent, the specification of a mechanism to control forwarding of event reports, the ability for an external managing system to modify conditions used in the reporting of events, and the ability to designate a backup location to which event reports can be sent if the primary location is not available. For details on each of these capabilities see the ERMF standard [ERMF].

3.3.6. Log Control Function (LCF)

The Log Control Function (LCF) specifies a particular management function and services which allow logging of information about event reports, notifications and operations performed by and on various objects. The event reports are presented directly to be processed for logging. The notifications are pre-processed to form potential log reports. Both the log records to be stored, and the logs in which they are stored, are modelled as managed objects. The LCF provides the services to initiate, terminate, suspend, or resume the activity of logging through the manipulation of the log object. The LCF supports retrieving log attributes values, notification of log attribute value changes, log record retrieval, and log record deletion. For details on the selection of information to be logged, see the LCF standard [LCF].

3.3.7. Security Alarm Reporting Function (SARF)

While alarm notifications of a general type are considered to be under the scope of the ARF, certain types of alarm notifications need different handling. The security Alarm Reporting Function (SARF) specifies a particular form for notifications of security related events. The SARF standard defines five types of security alarms and eighteen registered security alarm causes. The standard also defines three parameters used to identify the cause of security breaches. For details on these parameters, each of the alarm types, and the causes which are assigned to individual alarm types, see the SARF standard [SARF].

3.4. Management Security

3.4.1. Services

The GOSIP identifies the primary services required for security in an open system. These services are:

- authentication (verifies the identity of communicating peer entities),
- access control (allows only authorized communication and system access),
- data confidentiality (protects data against unauthorized access),
- data integrity (protects data against unauthorized modification, insertion, and deletion), and
- non-repudiation (provides proof of the origin or receipt of data).

The OIW Network Management Special Interest Group (NMSIG) has identified the following security services, as qualified below, as the primary requirements for network management security:

- authentication - peer entity and data origin authentication,
- access control,
- confidentiality - connectionless confidentiality, and
- integrity - connectionless integrity.

Since not all systems will require all the security services, and not all these services will be available in the immediate future, the NMSIG has prioritized these services with regard to their general usefulness and urgency. Highest priority has been given to access control. In addition, because access control is so closely related to and dependent upon authentication, authentication was also given a high priority (i.e., it must be verified that a person or process is in fact, who it claims to be, before granting it access to a protected system or object).

3.4.2. Authentication

Various standards bodies are developing specifications for incorporating security services within OSI protocols. As appropriate specifications emerge they will be applied to network management and other application layer protocols. To accommodate current security needs prior to standards reaching full maturity, Version 1 GNMP specifies two modes of authentication between which Acquisition Authorities may choose. Specification of security requirements is optional in a Request for Proposal (RFP). If required, the Acquisition Authority shall select only one of the two modes of authentication. Version 1 GNMP strongly recommends that the Acquisition Authorities requiring optional authentication service specify Mode 2.

Both modes use simple credentials, as defined in the Directory Authentication standard [DDEF], to authenticate an entity requesting the establishment of a management association. The simple credentials structure comprises the following fields: username, password, optional time-stamp, and optional random number. The time-stamp fields and random number fields may be used to protect against replay attacks. A detailed description of each of the two authentication modes follows.

Mode 1: Mode 1 authentication requires use of the username and password fields of the simple credentials. This method uses the extensions to the Association Control Service Element (ACSE) service and protocol standards [ACSES] [ACSEP] which define a new functional unit (authentication) in which this information is conveyed. An authenticating entity must compare the username and password against an "authorized users" list to verify the user's identity. If the identity is confirmed, the association is accepted; otherwise, it is rejected. The username and password are the minimum amount of information that must be provided for Mode 1 authentication. The password is transmitted in the clear, not encrypted

in any way. Distribution method for the usernames and passwords is dependent upon prior agreements between communicating peer entities, and is, therefore, beyond the scope of the GNMP.

Mode 2: In addition to providing all aspects of Mode 1 authentication, Mode 2 authentication provides additional security by using a hash function applied to the authentication information (e.g., the password). A time-stamp may be included in the authentication information, to which the hash function is applied, to provide a greater measure of security (i.e., by adding the time-stamp, the password will hash to a different value each time). For Mode 2 authentication, the Secure Hash Algorithm (SHA) specified in [SHA] must be supported for government use. Other hash algorithms may also be supported (e.g., the MD5 algorithm specified in part 12, clause 7.2.3 of the June 1992 SIAs [STABLE].) An authenticating entity receives the hashed output in the password field of the simple credentials structure, and then processes the password "known" locally to correspond to the received username (along with the other authentication information as the requesting entity did) using the hash function to produce a test value. This test value and the password field are then checked for equality. If the user identity is authenticated, the association is accepted; otherwise, it is rejected. The distribution of the password used as input for hashing is dependent upon prior agreements between communicating peer entities, and is, therefore, beyond the scope of the GNMP.

3.4.3. Access Control

For Version 1 GNMP, the access control policy is as follows: once authenticated on an association, an entity shall have access to all management information available through that association. If an entity is not authenticated, it will not be granted an association.

As work progresses on access control in the standards community, access control mechanisms will be added to future versions of the GNMP.

3.4.4. Remaining Services

For Version 1 GNMP, data origin authentication, integrity, and confidentiality are not specified. As work progresses on these services in the standards community, they will be added to future versions of the GNMP.

4. GNMP Conformance Requirements

Implementations may be conformant to the Government Network Management Profile (GNMP) in any of three areas:

- management communications,
- management information, and
- systems management functions.

An implementation may be conformant to one or more of these areas. When purchasing implementations, Acquisition Authorities shall specify the areas to which conformance is required. If management security is required, an implementation shall be conformant to one of the two peer-entity authentication modes as described in Section 3.4.2 of this document. Inclusion of security features in an RFP is optional.

When procuring a complete Network Management System (NMS), the Acquisition Authority should take additional steps, as recommended in section 2 of the GNMP, to ensure an adequate specification for the intended use of the NMS. For example, considerable attention should be given to the human-machine interface (HMI) and the analysis needs, since such functionality is usually required.

4.1. Management Communications Conformance Requirements

To be conformant with the GNMP in the area of management communications, an implementation shall satisfy the requirements for management communications as stated in part 18, clause 8.3.1 of the June 1992 SIAs [STABLE]. An implementation shall, also, provide the ACSE services and protocol as specified in GOSIP Version 2, section 4.2.7.1, as modified by the NMSIG Agreements (part 18 of OIW SIAs), clause 6.5. In addition, an implementation shall provide the ROSE services and protocol as specified in the Remote Operations Part 1: Model, Notation and Service Definition [ROSES], and the Remote Operations Part 2: Protocol Specification [ROSEP], and as modified by the NMSIG Agreements clause 6.5. Agreements relating to the presentation and session layers shall also be supported as specified in the Upper Layer Agreements, part 5, clause 13.7 of the June 1992 OIW Stable IAs, [STABLE]. The particular combination of allowable layer 1-6 services and protocols selected to support CMIS/P protocols/options shall be dictated by the intended network management applications and by the target network(s).

Note: If VT functionality is required, VT should be specified as stated in the GOSIP Version 2 section 4.2.7.4 [GOSIP].

If FTAM functionality is required, FTAM should be specified as stated in the GOSIP Version 2 sections 4.2.7.2 and 5.3.1 [GOSIP].

If MHS functionality is required, MHS should be specified as stated in the GOSIP Version 2 sections 4.2.7.3, and 5.3.2 [GOSIP].

4.2. Management Information Conformance Requirements

To be conformant with the GNMP in the area of management information, an implementation shall include at least one managed object (MO). Where applicable, managed objects shall be selected from the MO definitions in the following standards documents and implementation agreements.

The standards documents include:

- Definition of Management Information [DMI]
- IEEE 802.1B LAN/MAN Management [L/MAN]
- IEEE 802.3 Repeater Management [HUB]
- ANSI X3T9.5 FDDI Station Management [FDDI]
- CCITT Generic Network Information Model [CCITT]
- ISO/IEC JTC1/SC6 Management Information Related to OSI Network Layer Standards [NW]
- ISO/IEC JTC1/SC6 Management Information Related to Intermediate System to Intermediate System Intra-Domain Routing Information Exchange Protocol [ISIS]
- ISO/IEC JTC1/SC6 Management Information Related to OSI Transport Layer Standards [XPORT]

The implementation agreements include:

- Annexes A and B of part 18 (NM IAs) of OIW Stable IAs, June 1992 [STABLE]
- The Network Management Forum Management Information Library [NMFMIL]

When specifying MOs in an RFP for NM products, the Acquisition Authority shall take care to specify: 1) from which document the MOs are selected, since MO names need only be unique within a particular defining document and may, therefore, be similar or identical to names of different objects in other documents; 2) whether, and which, optional attributes and/or conditional package(s) are mandatory for the procurement; and 3) at least one name binding for each of the MOs selected.

In those cases where applicable MOs cannot be found in the above listed documents for managing particular network component(s) or system(s), additional, more appropriate managed objects may need to be defined. The definitions of such managed objects shall satisfy the requirements for management information as stated in part 18, clause 8.3.3 of the OIW SIAs, June 1992, [STABLE]. The techniques and templates specified in the Guidelines for the Definition of Managed Objects (GDMO) [GDMO] shall be used in defining these MOs. When defining MOs, two steps should be taken to assure that the management information base is kept

as lean and coherent as possible. First, the management information documents listed above, plus those SMFs stated in Section 3, should be thoroughly searched to assure that an appropriate MO has not already been defined for the desired purpose. Then, these same documents should be searched for an already defined MO which, although not entirely satisfactory, may be sufficiently close to the desired MO so that it could serve as a super class from which this new object class could be derived. Elements of MOs (e.g., attributes or notifications) should be handled in the same manner to prevent redundant definition of similar or identical management information elements. All MO definitions must have registered object identifiers and must be publicly available.

The initial issue of the management information catalogue [MICAT] jointly published by NIST, the OIW NMSIG and the NMF is a reference document intended to enable individuals or organizations to quickly and easily identify information related to their network management activities. The catalogue makes easily visible the full repertoire of management information defined and available at a given point in time. This catalogue may be used to assist Acquisition Authorities in identifying additional applicable managed object definitions.

4.3. Systems Management Functions Conformance Requirements

To be conformant with the GNMP in the area of systems management functions, an implementation shall satisfy the requirements for systems management functions as stated in part 18, clause 8.3.2 of the OIW Stable IAs, June 1992 [STABLE].

The Acquisition Authority, when specifying systems management functions (SMF) in an RFP for NM products, shall take care to select the applicable SMF categories as specified in part 18, clause 8.3.2 of the June 1992 OIW Stable IAs [STABLE]. The SMF categories include:

- General Management Capabilities,
- Alarm Reporting and State Management Capabilities,
- Alarm Reporting Capabilities,
- General Event Report Management Capabilities, and
- General Log Control Capabilities.

The Acquisition Authority, when specifying the selected SMF categories in the RFP, shall specify the selected functional units and shall specify whether conformance to the agent role, the manager role, or both, is required.

4.4. Peer-entity Authentication Conformance Requirements

To be conformant with the GNMP in the area of peer entity authentication, one of the two authentication modes as described in Section 3.4.2 of this profile shall be specified. In both modes, an Application Layer function shall be performed during association establishment, and

shall be accomplished using ACSE extensions [ACSES] and [ACSEP]. These extensions define a new functional unit and the associated ASN.1 definition of an "authentication" parameter to support authentication. If any mode of authentication is selected for use by the Acquisition Authority, the implementor shall implement the two ACSE extensions [ACSES][ACSEP]. In addition, the implementation shall use Simple Credentials as defined in the Directory Authentication Framework Part 3 [DDEF], for use in the authentication field of the protocol data unit as specified in [ACSEP]. The implementation shall follow the method of simple authentication as defined in the Directory Authentication Framework Part 8, Section 2 [DAUTH]. Since the Directory is not mandatory, the authentication functionality (e.g., checking of password for equality) shall be performed by the authenticating entity. In both authentication modes, password usage shall conform to FIPS 112, Password Usage [PASS]. In both modes, the distribution of the usernames and passwords is dependent upon prior agreements between authenticating peer entities and is, therefore, beyond the scope of the GNMP.

5. Testing of GNMP-compliant Implementations

5.1. Conformance Testing

Systems Management is expected to be added to the GOSIP testing program; therefore, demonstration of conformance to GNMP will be possible. To demonstrate conformance implies product testing in an accredited testing laboratory, and registration in the Conformance Tested GOSIP Product Register. The testing program will identify and register abstract test suites, and will assess and qualify Means of Testing.

5.2. Interoperability Testing

Interoperability testing for the GNMP should be strongly considered. Possibilities for such testing include the use of commercially available interoperability testing services, or on-site multi-vendor testing to assure interoperability. The list of recognized interoperability services will be available in the Interoperability Test and Registration Service Register of the GOSIP Register Database, and minimum required interoperability test suites will be identified and registered by the U.S. GOSIP Testing Program.

Appendices

A. Advanced Requirements

This appendix provides a forward pointer to additional work planned for subsequent versions of the GNMP.

A.1. Management Information

For the definitions of management information, Version 1 GNMP focuses primarily on identifying the information required for managing implementations incorporating the functionality specified for layers 1-2 of the OSI Reference Model [BRM].

The second Version of the GNMP, planned to be released approximately eighteen months after Version 1 GNMP is promulgated, will mainly add the information required for managing implementations of the functions specified for layers 3-7 of the OSI reference model. Version 3 will specify the management information (MI) required for the management of computer applications and services that are outside of the 7-layer communications stack, such as computer operating systems and database management systems.

A.2. Systems Management Functions

The inclusion of the Systems Management Functions (SMFs) for subsequent versions of the GNMP is to be in accordance with the status of the management standards and of the IAs; that is, as the SMFs mature and implementors agreements are reached on the SMFs, they will be considered for inclusion in the GNMP. For example, standards are now under development to specify how managing and managed systems are to share management knowledge needed and used in common. These specifications will be referenced in the GNMP as they become available as international standards.

A.3. Management Security

Version 1 GNMP specifies two optional peer-entity authentication modes. Work on Access Control, Confidentiality, Integrity, and Nonrepudiation standards is still in its infancy, but these issues will be addressed in future versions of the GNMP. The goal of the GNMP is to provide all necessary security services to address the security needs of network management.

A.4. The Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) is widely implemented and is likely to be deployed to manage routers. In such deployments, SNMP can be viewed, analogously to proprietary network management protocols, as an internetwork management protocol (i.e., for managing sets of routers). Thus, the SNMP can be fitted into a network management architecture that also includes the GNMP protocols. Providing such a capability (i.e., to integrate the GNMP and the SNMP into a single network management system) is a future work item for the GNMP.

A.5. NM Ensembles

A recently developed concept related to the selection of managed objects (MOs) and system management functions (SMFs) that solves a particular management problem is the concept of "ensembles." Currently, an ensemble is defined as a coherent unit that specifies: 1) the particular problem to be solved, the requirements associated with the problem and a solution to the problem; and 2) the standards and MOs making up the solution. This concept was developed by the Architecture Team of the Network Management Forum (NMF). The Object Team of the NMF is developing specific ensembles (e.g., the OSI Interworking Ensemble and the Reconfigurable Circuit Service: Configuration Management (RCS) Ensemble). While more work needs to be done, the concept appears to have great merit and offers potential for assisting in the preparation of RFPs for NM products. As the ensembles concept and the definitions of the ensembles mature and stabilize, consideration will be made on whether or not to include ensembles in later versions of the GNMP.

B. Where to get Documents

The technical specification of V.1 GNMP is available both on-line and in hardcopy.

hardcopy: National Technical Information Service (NTIS)
U. S. Department of Commerce
5285 Port Royal Road
Springfield, VA 22161.
(703) 487-4650

on-line. available from osi.ncsl.nist.gov via anonymous ftp (129.6.48.100) or anonymous ftam: type "ftamosi"

./pub/gnmp/gnmp.asc	--- ascii
./pub/gnmp/gnmp.ps	--- PostScript
./pub/gnmp/gnmp.w51	--- Wordperfect 5.1

Note: PostScript figures are in the files in the same subdirectory as figN.ps where N = 1, 2, 3.

The Stable Implementation Agreements (SIA) for Open Systems Interconnection Protocols (NIST Special Publication 500-202) is also available both on-line and in hardcopy.

hardcopy: National Technical Information Service (NTIS)
U. S. Department of Commerce
5285 Port Royal Road
Springfield, VA 22161.
(703) 487-4650.

This document may also be purchased from the IEEE Computer Society. Order Department, Phone: 1-800-272-6657.

on-line: available from osi.ncsl.nist.gov via anonymous ftp (129.6.48.100) or anonymous ftam: type "ftamosi"

./pub/oiw/agreements/XS-9112.asc	--- ascii
./pub/oiw/agreements/Xs-9112.w51	--- Wordperfect 5.1

The addresses and telephone numbers that may be used to obtain additional GNMP-related documents are listed below.

IEEE Computer Society Press
Order Department
10662 Los Vaqueros Circle
Los Alamitos, Ca. 90720
1-800-272-6657

Network Management Forum
40 Morristown Rd.
Bernardsville, NJ 07924
TEL:(908)-766-1544
FAX:(908)-766-5741

American National Standards Institute
11 W. 42rd St.
N.Y., N.Y. 10036
TEL:(212)642-4900
FAX:(212)302-1286

International Organization for Standardization
Central Secretariat
Case postale 56-CH-1211
Geneve 20, Switzerland
TEL:41 22 749 01 11
FAX:41 22 733 34 30

National Technical Information Service (NTIS)
U. S. Department of Commerce
5285 Port Royal Road
Springfield, VA 22161.
(703) 487-4650.

CCITT
International Telecommunications Union
Place des Nations
CH 1211
Geneve 20 SWITZERLAND

C. Acronyms

ACSE	Association Control Service Element
ANSI	American National Standards Institute
ARF	Alarm Reporting Function
ARR	Attributes for Representing Relationships
ASE	Application Service Element
CCITT	International Telegraph and Telephone Consultative Committee
CMIP	Common Management Information Protocol
CMIS	Common Management Information Services
DIS	Draft International Standard
DMI	Definition of Management Information
ERF	Event Report Function
FDDI	Fiber Distributed Data Interface
FIPS	Federal Information Processing Standard
FTAM	File Transfer, Access, and Management
GDMO	Guidelines for the Definition of Managed Objects
GNMP	Government Network Management Profile
GOSIP	Government Open Systems Interconnection Profile
HMI	Human Machine Interface
IA	Implementor's Agreement
IEEE	Institute of Electrical and Electronic Engineers
IGOSS	Industry/Government Open Systems Specification
IS	International Standard
ISO/IEC	International Organization for Standardization/International Electrotechnical Committee
LAN	Local Area Network
LCF	Log Control Function
MAP	Manufacturing Automation Protocol
MHS	Message Handling Systems
MIL	Management Information Library
MIM	Management Information Model
NIST	National Institute of Standards and Technology
NM	Network Management
NMS	Network Management System
NMSIG	Network Management Special Interest Group
OIW	OSE Implementors Workshop
OMF	Object Management Function
OSE	Open Systems Environment
OSI	Open Systems Interconnection
RFP	Request For Proposal
SARF	Security Alarm Reporting Function
SATF	Security Audit Trail Function

SIG	Special Interest Group
SMFs	Systems Management Functions
SMFAs	Specific Management Functional Areas
SMI	Structure of Management Information
SMO	Systems Management Overview
SNMP	Simple Network Management Protocol
STMF	State Management Function
TOP	Technical and Office Protocols TMF
VT	Virtual Terminal
WAN	Wide Area Network

D. Glossary

The terms defined below are used frequently throughout this profile and are defined here to aid the reader. The OSI Basic Reference Model, [BRM], may be referenced for other terms appearing in this document.

Acquisition Authority	An individual or team who, under Federal law and acquisition regulations, has the authority to enter into, administer, and/or terminate a government contract.
Agent	A management information services user making use of systems management services, which, for a particular exchange of systems management information, has taken an agent role.
Agent Role	A management information services user making use of systems management services, taking an agent role is capable of performing management operations on managed objects and of emitting notifications on behalf of managed objects.
Allomorphism	The ability of a managed object that is an instance of a given class to be managed as an instance of one or more other managed object classes.
Containment	A relationship between managed object instances (not between managed object classes) used for naming managed objects.
Inheritance	The conceptual mechanism by which attributes, notifications, operations and behavior are acquired by a subclass from its superclass.
Managed Object (MO)	The OSI management view of a resource that is subject to management, such as a layer entity, a connection or an item of physical communications equipment. A managed object is the abstracted view of such a resource that represents its properties as seen by (and for the purposes of) management.
Managed Object Class	A named set of managed objects sharing the same set of attributes, notifications, and management operations.

Manager	A management information services user making use of systems management services, which, for a particular exchange of systems management information, has taken a manager role.
Manager Role	A management information services user making use of systems management services, taking the manager role is capable of issuing management operations and of receiving notifications.
Notification	Information emitted by a managed object relating to an event that has occurred within the managed object.
OSI Management	The facilities to control, coordinate and monitor the resources which allow communications to take place in the OSI environment.
Protocol	In the Open System Interconnection Reference Model, the communication functions are partitioned into seven layers. Each layer, N, provides a service to the layer above, N+1, by carrying on a conversation with layer N on another processor. The rules and conventions of that N-layer conversation are called a protocol.
Requests For Proposals (RFP)	Requests For Proposals are documents issued by the government to request bids for products or services.

References

[ACSES] *"Information technology - Open Systems Interconnection - Service Definition for the Association Control Service Element, Amendment 1: Peer-entity Authentication during Association Establishment,"* ISO/IEC 8649 Amd1:1990.

[ACSEP] *"Information technology - Open Systems Interconnection - Protocol Specification for the Association Control Service Element, Addendum 1: Peer-entity Authentication during Association Establishment,"* ISO/IEC 8650 Amd1:1990.

[ALS] *"Information technology - Open Systems Interconnection - Application Layer Structure,"* ISO/IEC 9545, September 1988.

[ARF] *"Information technology - Open Systems Interconnection - Systems Management - Part 4: Alarm Reporting Function,"* CCITT Rec. X.733 | ISO/IEC IS 10164-4, 1991.

[ARR] *"Information technology - Open Systems Interconnection - Systems Management - Part 3: Attributes for Representing Relationships,"* CCITT Rec. X.732 | ISO/IEC IS 10164-3, 1991.

[BRM] *"Information technology - Open Systems Interconnection - Basic Reference Model,"* ISO/IEC 7498, 1984.

[CCITT] *CCITT Draft Recommendation (M.3100) Generic Network Information Model,* November 1991.

[CMIP] *"Information technology - Open Systems Interconnection - Management Information Protocol Specification - Common Management Information Protocol,"* CCITT Rec. X.711 | ISO/IEC 9596-1, 1991.

[CMIS] *"Information technology - Open Systems Interconnection - Management Information Service Definition - Common Management Information Service Definition,"* CCITT Rec. X.710 | ISO/IEC 9595, 1991.

[DAUTH] *"Information Technology - Open Systems Interconnection - The Directory - Part 8: Authentication Framework,"* ISO/IEC 9594-8:1988.

[DDEF] *"Information Technology - Open Systems Interconnection - The Directory - Part 3: Abstract Service Definition,"* ISO/IEC 9594-3:1988.

[DMI] *"Information technology - Open Systems Interconnection - Structure of Management Information - Part 2: Definitions of Management Information,"* CCITT Rec. X.721 | ISO/IEC IS 10165-2, 1991.

[ERMF] *"Information technology - Open Systems Interconnection - Systems Management - Part 5: Event Report Management Function,"* CCITT Rec. X.734 | ISO/IEC IS 10164-5, 1991.

[FDDI] *"FDDI Station Management, Rev. 7.2"* Preliminary Draft Proposed American National Standard, 1992.

[FRMWK] *"Information technology - Open Systems Interconnection - Basic Reference Model - Part 4: Management Framework,"* ISO/IEC 7498-4, 1989.

[GDMO] *"Information technology - Open Systems Interconnection - Structure of Management Information - Part 4: Guidelines for the Definition of Managed Objects,"* CCITT Rec. X.723 | ISO/IEC IS 10165-4, 1991.

[GMI] *"Information technology - Open Systems Interconnection - Structure of Management Information - Part 5: Generic Management Information,"* ISO/IEC DIS 10165-5, February 1992.

[GOSIP] *"Federal Information Processing Standards Publication 146-1, U.S. Government Open Systems Interconnection Profile (GOSIP),"* National Institute of Standards and Technology, 3 April 1991.

[HUB] *"Draft Supplement to ANSI/IEEE Std. 802.3 - 1992 Edition, Repeater Management,"* P802.3 K/D10, July 11, 1992.

[ISIS] *"Information technology - Telecommunications and information exchange between systems -- Intermediate system to Intermediate system Intra-Domain routing information exchange protocol for use in conjunction with the Protocol for providing the Connectionless-mode Network Service (ISO 8473),"* ISO/IEC 10589, 1992.

[LCF] *"Information technology - Open Systems Interconnection - Systems Management - Part 6: Log Control Function,"* CCITT Rec. X.735 | ISO/IEC IS 10164-6, 1991

[LMAN] *"Draft Standard 802.1B : LAN/MAN Management,"* P802.1B/D20, January 27, 1992.

[MICAT] *"Management Information Catalogue,"* Issue 1.0, June 1992, published by NIST, Network Management Forum and Open Systems Environment Implementors' Workshop Network Management Special Interest Group.

[MIM] *"Information technology - Open Systems Interconnection - Management Information Services - Structure of Management Information - Part 1: Management Information Model,"* CCITT Rec. X.730 | ISO/IEC IS 10165-1, 1991.

[MOCS] *"Information technology - Open Systems Interconnection - Structure of Management Information - Part 6: Requirements and Guidelines for Implementation Conformance Statement Proformas Associated with Management Information,"* ISO/IEC CD 10165-6, 21 February 1992.

[NMFMIL] Network Management Forum: Forum 006, *"Forum Library - Volume 4: OMNIPoint 1 Definitions,"* Issue 1.0, August 1992.

[NW] *"Information technology - Telecommunications and information exchange between systems -- Elements of Management Information Related to OSI network Layer Standards,"* ISO/IEC IS 10733 (Approved July 1992, to be published)

[OMF] *"Information technology - Open Systems Interconnection - Systems Management - Part 1: Object Management Function,"* CCITT Rec. X.730 | ISO/IEC IS 10164-1, 1991.

[PASS] *"Federal Information Processing Standards Publication 112, Password Usage,"* National Institute of Standards and Technology, May 1985.

[ROSEP] *"Information technology - Text Communications - Remote Operations Part 2: Protocol Specification,"* ISO/IEC 9072-2, 19 September 1989.

[ROSES] *"Information technology - Text Communications - Remote Operations Part 1: Model, Notation and Service Definition,"* ISO/IEC 9072-1, 19 September 1989.

[SARF] *"Information technology - Open Systems Interconnection - Systems Management - Part 7: Security Alarm Reporting Function,"* CCITT Rec. X.736 | ISO/IEC IS 10164-7, 1991.

[SHA] *"Specifications for a Secure Hash Standard"*, the proposed Federal Information Processing Standard, January 22, 1992. (available from NIST)

[SMO] *"Information technology - Open Systems Interconnection - Systems Management Overview,"* CCITT Rec. X.701 | ISO/IEC IS 10040, 1991.

[STABLE] NIST Special Publication 500-202, *"Stable Implementation Agreements for Open Systems Interconnection Protocols, Version 5 Edition 1."*

[STMF] *"Information technology - Open Systems Interconnection - Systems Management - Part 2: State Management Function,"* CCITT Rec. X.731 | ISO/IEC IS 10164-2, 1991.

[XPORT] *"Information technology - Telecommunications and information exchange between systems -- Elements of Management Information Related to OSI Transport Layer Standards,"* ISO/IEC IS 10737 (Approved July 1992, to be published)