NBSIR 87-3593

A Survey of OSI Network Management Standards Activities

C. Michael Chernick, Kevin Mills, Robert Aronoff,
John W. Strauch

U.S. DEPARTMENT OF COMMERCE
National Bureau of Standards
Institute for Computer Sciences and Technology
Gaithersburg, MD 20899

July 1987

U.S. DEPARTMENT OF COMMERCE
NATIONAL BUREAU OF STANDARDS

NBSIR 87-3593

A SURVEY OF OSI NETWORK MANAGEMENT STANDARDS ACTIVITIES

C. Michael Chernick, Kevin Mills, Robert Aronoff,
John W. Strauch

U.S. DEPARTMENT OF COMMERCE
National Bureau of Standards
Institute for Computer Sciences and Technology
Gaithersburg, MD 20899

July 1987

U.S. DEPARTMENT OF COMMERCE, Clarence J. Brown, *Acting Secretary*
NATIONAL BUREAU OF STANDARDS, Ernest Ambler, *Director*

A Survey of OSI Network Management Standards Activities

C. Michael Chernick

Kevin Mills

Robert Aronoff

John W. Strauch

July 17, 1987

CONTENTS

1 Executive Summary

This report is produced under contract #OCH-4-001 for the Air Force ULANA (Unified Local Area Network Architecture) Program Office. The report surveys OSI Network Management Standardization efforts with particular emphasis on those aspects of most interest to ULANA (e.g., local area networks). It reflects the status of OSI network management standardization efforts up to March, 1987. It builds upon a related paper "Status: Standardizing Management of OSI Networks" [BRUS87]. This executive summary contains the most important conclusions from the survey. The summary assumes the reader is familiar with OSI network management concepts. An introduction to these concepts is included as Section 2.3 of the main body of the report. The executive summary describes the outlook for network management standardization, identifies problems and concerns, and presents a time table for standardization and commercial product development.

1.1 Network Management Standards Outlook

Establishment of an internationally agreed set of network management standards for open systems interconnection is likely to occur. The first set of standards is likely to emerge in 1988, with the additional sets scheduled to appear through 1990. Several potential problems, discussed in the next section, may delay the process, but no obstacle will delay the standards indefinitely.

1.2 Network Management Standards Problems

During the survey of network management standardization, six potential problems were discovered. Each problem is discussed in order of the potential for adverse effect on the standards making process.

First, the General Motors' led Manufacturing Automation Protocol (MAP) standard setting process has placed a high priority on the specification of network management standards for inclusion in release 3.0 of MAP (scheduled for June 1987). The MAP 3.0 specification is based on the current immature international standards: however, MAP 3.0 will be implementable, while the corresponding international standards will not be implementable before 1989. Vendors may implement MAP 3.0 standards in 1988 leading to outdated products by 1989. Thus, there is some potential for MAP to set de facto network management standards incompatible with the international standards. This is unlikely to occur because MAP is publicly committed to adoption of international standards and because the Corporation for Open Systems (COS), a consortium of major computer and communications vendors, will probably lobby for a single set of network management standards applicable to OSI, MAP, and the Technical and Office Protocols (TOP).

The second potential problem involves the delay in the specification of the resource attributes to be managed. At each layer, resources exist that must be monitored and controlled to effect the management of the layer. Furthermore, because of the unique nature of each resource and its attributes, specific, unique actions may be defined for each.

The process of identifying resources and attributes, as well as allowed actions on them is the responsibility of the standardization group assigned to develop the protocols for that layer (e.g., Accredited Standards Committee (ASC) X3S3.3 is primarily responsible for the Transport and Network layers). has been slow to begin. An exception to this is the IEEE 802 committees which have completed much of this identification process, but only for the lower two layers of IEEE 802 defined Local Area Network (LAN) types. Any further delay in the identification process will likely result in future delays of product delivery.

The third potential problem involves the specification of underlying services for transfer of network management protocol data units (PDUs). The present set of standards defines a connection-oriented (CO) Remote Operation Service (ROS) to support the common management information protocol (CMIP). (ROS is a service within the application layer defined for the purpose of associating a result response from a remote system with a previous local invoking request.) There is a set of organizations supporting a connectionless (CL) ROS for the CMIP. CO vs. CL arguments have occurred in almost every OSI standard development effort. This argument may slow the development of the standards.

Another ROS issue is selection of an appropriate class of ROS functions to support CMIP. Today, the CMIP assumes that a supporting ROS implements the most general class of functions available. However, the ROS now defined provides a minimal class of functions. A complicating factor is that a number of organizations have questioned whether CMIP should use ROS services at all. The controversy surrounding these issues may delay the development of a stable CMIP standard.

The uncertainties with the ROS standard, which CMIP relies upon, lead to uncertainties in the CMIP specification. A continually changing CMIP will require extra work and may delay the development of a standard.

The fourth problem area concerns the definition of network mangement operations for network nodes with less than seven protocol layers, for example, intermediate systems, mini-MAP nodes and media access control level bridges. The current OSI network management standards assume all nodes contain a full seven layers of protocols. This is an unrealistic assumption and, therefore, an accommodation must be made in the standards. This accommodation will require more work and may delay the development of the standards.

The fifth problem concerns the management of implementation dependent resources that affect OSI performance. The present standards permit monitoring and control of OSI resources, but not of the implementation dependent resources necessary to affect performance. If the standards are modified to enable control of implementation dependent resources, great difficulty will be encountered identifying the resources subject to control. Such an attempted modification would delay the development of the management standards.

The sixth problem concerns local area network security. Little in the way of security has been defined for OSI protocols, particularly with respect to local area networks. Because they usually operate in a broadcast mode, LANs are particularly sensitive to problems in assuring data transfer confidentiality. Thus, the development of standards for OSI security management are dependent upon the definition of the actual OSI security standards. This may delay the development of the security management standards.

1.3 Network Management Standards Timetable

This section provides a timetable for progression of the core OSI network management standards under development within ASC X3T5.4 and ISO TC97/SC21/WG4. Related standards from groups such as ASC X3T5.5, ASC X3T5.1, IEEE 802, and ASC X3S3.3, are not specifically covered; however, such related layer management standards are likely to be available within the same time as the core standards. The time table for the core standards is given below.

1.3.1 Table of Priorities and Target Dates

This table is adapted from one in the "Report of the Second SC 21/WG4 Meeting" [SC21RP] and is ISO TC97/SC21/WG4's plan for progression to International Standards for various aspects of network management. The document reference numbers given under REF are those assigned by TC97/SC21. For those documents that have reached the status of Draft Proposed (DP) standard, the DP number is also given.

Title	REF	DP	DIS	IS
OSI Management Framework (DP7498/4)	N1371	9/86	9/87	9/88
OSI Management Information Service and Protocol				
Part 1 - Overview (DP9595/1) (DP9596/1)	N1372 N1374	9/86	9/87	9/88
Part 2 - Common Management (DP9595/2) (DP9596/2)	N1373 N1375	9/86	9/87	9/88
Part 3 - Fault Management	N1383 N1384	2/88	2/89	2/90
Part 4 - Accounting Management	N981	11/88	11/89	11/90
Part 5 - Configuration Management	N1385	2/88	2/89	2/90
Part 6 - Performance Management	N983	11/88	11/89	11/90
Part 7 - Security Management	N1386	2/88	2/89	2/90

1.4 Network Standards Commercial Product Availability

Commercial product availability is difficult to predict: however, previous experience with OSI products can be used as a guide. Vendors will generally begin product development when a standard reaches the Draft International Standard (DIS) state. Initial products are available within about two years of a standard reaching DIS. Sometimes the first products are not very stable, requiring another year to gain stability. Therefore, commercial products are usually available within two to three years of an OSI standard reaching the DIS state.

Using the previously presented network management standards timetable as a guide, one can expect stable commercial products for OSI network management to appear starting in 1989 and to evolve to a complete set of products by 1992. Delays in the standards setting process will directly delay the availability of commercial products.

2 Introduction

2.1 Review of the OSI Reference Model

The OSI Reference Model [IS7498] is, by now, a well known methodology for describing vendor independent communications between computing systems. The model divides the communications task into seven layers (Figure 1). Each layer contributes its additional functionality to the communications task. For example, the Network Layer provides for end-to-end routing of messages, while the Link Layer provides for communications across a single physical connection.

Each layer provides services at its upper layer interface (to the layer above it) that are usually described by a service specification for the layer. (The upper layer interface is also known as the service interface, as shown in Figure 1 for the Transport and Link layers.) These services at each layer are provided by an implementation termed a layer entity. Each layer entity communicates with its peer on another system using peer to peer protocols to provide the services specified in its service specification. This protocol is usually described by a protocol specification.

In some instances, a layer may be divided into sublayers. (Note: The term "sublayer" is now in disfavor by ASC X3T5.1, the committee concerned with OSI architecture. However, "sublayer" appears in at least one draft standard document.) There are several reasons for this. Often a layer needs a special sublayer to handle the service interface of the layer beneath it, thus avoiding a potential "rewrite" of the entire layer. For example, in the case of several of the IEEE 802 Local Area Network (LAN) standards, the Link Layer is divided into a Logical Link Control (LLC) sublayer and a Media Access Control (MAC) sublayer. The MAC sublayer is dependent upon characteristics of the underlying physical layer. Some Transport Layers include a Subnetwork Dependent Convergence Function (a sublayer) that differs depending upon whether the Network Layer is connection-oriented or connectionless.

Another type of sublayer is found within the Application Layer. Here, families of Application Service Elements (ASEs) may appear to support functionality required by several types of applications. Examples of ASEs include Concurrency, Commitment, and Recovery (CCR) and Association Control Service Element (ACSE).

To maintain layer independence and to promote modularity, layer entities on one system are not permitted to communicate with non-peers on another OSI system. Advantages of this scheme include ease of software maintenance and meaningful conformance testing. Another advantage is the ability to use the services of one layer independently of the lower layers. (For example, a Transport connection might be made without the user's knowledge of the underlying physical technology employed.)

In general, this peer-to-peer communication is accomplished by transmitting indivisible sequences of data called Protocol Data Units (PDUs). These are named for the layer whose services they provide. For example, Transport Layer PDUs are called TPDUs and Link Layer PDUs are called LPDUs. Generally, higher layer PDUs are embedded within lower layer PDUs. Thus TPDUs are sent within Network Layer PDUs (NPDUs), which are sent within LPDUs. (The Physical Layer is unusual in that it normally does not have PDUs of its own, but consists of mechanical and electrical signaling conventions.)

Certain aspects of layer entities are not specified in either the service or the protocol specification. These are called implementation dependent aspects and are beyond the scope of OSI standardization. Such aspects lead to differences between implementations. Sometimes these are related to inherent features of computer architectures. An example of this is the size of counters. On one system a 32-bit counter is implemented; on another, a 16-bit counter is the natural choice.

Often implementation differences are the result of an implementor's design decisions. A prime example (and one that can have a large effect on performance) is buffer management strategy. Another is acknowledgement strategy (used to confirm receipt of PDUs from one's peer entity). It is these differences in implementations that can often lead to one vendor producing a superior product compared to another.

A fundamental objective of the OSI concept is interoperability among diverse types of computing systems (both hardware and software). Although implementation differences can often cause performance differences, they may not cause conformance differences. Conformance can be evaluated by testing that stimuli presented at the upper layer, as required by the service specification, cause PDUs to be transmitted at the conceptual lower layer, as permitted by the protocol specification. Of course, the converse must be true. PDUs received at the lower layer must produce the proper stimuli at the upper layer interface. Implementations that meet these tests are termed Conforming Implementations.

An OSI conformant system can be considered to be composed of a set of resources. A resource is an entity that participates in the communications process. For example, a layer entity or an application process may each be considered to be a resource. Items of information about a specific resource are called attributes of the resource. [T54C87] In some OSI working papers, resource attributes are referred to as management objects or simply objects. [PFSM86] Objects may be conceptual or physical. Within a layer, many of these objects, e.g., timers, counters, and connection identifiers, are specified within the protocol or service specification for the layer. (At the physical layer management objects are often physical rather than conceptual and might include, for example, communications lines, modems, and line

controllers.) Normally some resource attributes, such as buffer allocation counters, are implementation dependent (i.e., not specified in either the service or protocol specification for the layer).

(Note: For consistency and to avoid confusion, the terms "resource attribute" or "attribute" will be used in the remainder of this report rather than "management object" or "object", with the understanding that the terms are synonymous. Also, terminology and concepts relating to resources and relationships among resources is still the subject of active discussion within the domestic and international standards making community. For a further discussion of these issues see Section 4.8, Management Information Base (MIB) and Structure of Management Information (SMI).)

2.2 Purpose of This Report

OSI Network Management (NM) will provide the means for monitoring and control of OSI resources. A management model has been developed [MGFM86] which describes the goals of NM in broad categories such as performance, configuration, and security. The resources to be managed may exist at one or several of the OSI layers. For each layer to be managed the resources and allowable operations that affect them must be identified. In addition, a protocol for communicating management information between OSI systems must be specified. This paper explains these concepts and reports on the progress of the major standardization groups developing and refining them.

2.3 Introduction to OSI Network Management Concepts.

Figure 2, "Simplified Functional Overview of OSI Network Management", illustrates some of the concepts to be developed in the OSI NM standardization process. Simply stated, the primary goal of this process is to provide the ability for an OSI network manager (probably a human, maybe an automated process) on an OSI system to monitor and control OSI resources within other systems on an OSI network. (Note: OSI resources are those concerned with the communications aspects of Open Systems, as opposed to systems resources which are of local concern only.) Furthermore, these other systems may be supplied by vendors other than the vendor which supplied the manager's system. In other words, the goal is to allow interoperability of network management products.

Figure 2 illustrates this point with three systems shown. The first, System "A" is supplied by vendor "X", the second, System "B" by vendor "Y", and the third, System "C", by vendor "Z". These systems are connected by an OSI network, which may be a Local Area Network (LAN), Wide Area Network (WAN), or some other type, perhaps using some technology not yet developed.

A manager, at a console on "A", can monitor resources being used within systems "B" and "C". If the manager determines that some adjustment may be needed to the resource attribute values, he may exercise control and modify the state of the resource. For example, he monitors the retransmission count of Link Layer PDUs (LPDUs, often referred to as "frames" or "packets") sent from "B" (shown as RETRAN_CNT) and determines that there are many more than expected for optimum performance. Therefore, the manager increases the retransmission timer (shown as RETRAN_TIM) on the assumption that delays somewhere in the network are causing the unnecessary retransmission of LPDUs. He may then continue to monitor the network to determine if this change corrected the problem.

OSI network management considers several broad categories of management objectives -- performance management, fault management, configuration management, security management, and accounting management. These objectives may sometimes conflict with one another. For example, security management may include overhead in LPDUs that reduce performance. Even within a management objective area, conflicting effects may be caused by a single management manipulation. For example, adjusting Transport parameters for optimal throughput, may, in some cases, adversely affect Network performance. It is up to the network manager to balance these objectives on each network.

2.4 Goal of OSI Standardization

This document is concerned with the status of OSI management standardization. It is important to note that the direct goal of OSI standardization as understood by the standards making community is NOT to provide tools or methods for managers of OSI systems. Rather, the goal of OSI standardization is to provide common standards such that implementors (usually, but not necessarily, OSI protocol vendors) can build tools that allow managers to manage OSI systems such that the tools provided by one implementor can interoperate with OSI resources on systems provided by another vendor or implementor. Thus, while different implementors network management products can interoperate, the products themselves may be quite different, consistent with the fact that interoperability among different products is the major design goal of OSI.

3 The OSI Management Model

This section provides an introduction to some of the concepts in the OSI management model. (These concepts are discussed in more detail below in Section 4, Components of Network Management. The ISO has developed an OSI management model within its Management Framework document [MGFM86], which was recently (September 1986) balloted as a draft addendum to the ISO Basic Reference Model [IS7498]. However, the document failed the ballot and will be revised in preparation for reballoting, probably

within the next six months.

Management in OSI is concerned with the monitoring and control of interconnection activities and OSI resources. To aid in the management activity, there is an Application entity called a System Management Application Entity (SMAE) at each system participating in the management process. Tools are required to allow for the exchange of information between OSI systems for management purposes in general and between cooperating SMAEs in particular.

A major tool is a protocol for exchange of information between management entities on OSI networks (e.g., between a system being managed and another system monitoring and controlling it.) The logical path taken by this information flow is shown in Figure 3, "Simplified OSI Management Model." This protocol is usually referred to as Common Management Information Protocol. (CMIP) [CMIPSP]. The services provided by this protocol are defined by the Common Management Information Service (CMIS) Specification [CMISSP].

There are several "management facilities" (essentially management objectives) defined in the OSI Management Framework document [MGFM86]. These include:

fault management,
accounting management,
configuration and name management,
performance management, and
security management.

These and other important concepts in the Management Framework are discussed in more detail below in Components of Network Management.

The resources being managed on an OSI system may exist at many layers of the OSI protocol stack, although the Application layer is often thought of as being outside the scope of OSI network management. Each layer to be managed requires a Layer Management Entity (LME). The LME provides an interface to the layer entity at that system. The LME communicates with the SMAE on the OSI system using implementation dependent techniques beyond the scope of OSI standardization. Development of layer management techniques for a given layer are generally the task of the developers of that layer as they are most familiar with the resources that need to be managed in the layer. For example, IEEE 802.3 has primary responsibility for LME development for the physical layer associated with 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) LANs.

4 Components of Network Management

The components of network management discussed here include a more thorough discussion of the Management Framework (MF) as well as a discussion of the OSI management Facilities.

4.1 Architecture/Framework

The primary architectural model used by the OSI standards community for network management is the one described in the MF document [MGFM86]. This is the base document by which OSI net management functionality will be discussed and to which other documents or techniques (e.g., IEEE System Management Revision L [IESMRL]) should be compared and contrasted.

The OSI MF document defines the scope of OSI management to include the following management facilities:

Fault Management
Accounting Management
Configuration and Name Management
Performance Management
Security Management

Each of these management facilities (sometimes referred to as Specific Management Information Services (SMIS)), are discussed further below in separate sections.

The Management Framework identifies categories of OSI resource management. There is systems management which encompasses mechanisms for management across multiple layers; (N)-layer management which is the management of a single layer; and (N)-layer operation which provides the management for a single instance of communication within the (N)-layer.

The Management Framework dictates that when an OSI system has all seven layers functional, then the facilities of system management should be used. Systems management functions on an open system are known as a Systems Management Application Processes (SMAP). That portion of an SMAP responsible for communication between SMAPs is known as a Systems Management Application Entity (SMAE). (See Figure 3.) Communications between SMAEs is accomplished through the use of the Common Management Information Protocol (discussed in more detail in another section below).

Note: The Management Framework document does not include a diagram of the management model. There apparently has been controversy within the management development community as how to best depict the inter workings among the management elements (e.g., SMAP, SMAE, layer managers). The model drawn in Figure 3 is a simplification presented on the thesis that a simple, drawing is better than none.

In some cases, for example, when a system is being down line loaded or the system to be managed is a relay or bridge, the full seven layers are not available. In such cases, the facilities of those lower (N)-layer management entities which are operational can be used, providing limited functionality. The exact nature of this limit is not clear from the Framework document so it remains to be seen how well this scheme will work, especially in cases

where a system with all seven layers attempts to manage one with a limited number of operational layers.

4.2 Common Management Information Service (CMIS) and Protocol (CMIP)

For OSI systems to cooperate for the purpose of network management, information must be exchanged between management processes on the different systems. To provide for these exchanges, ISO TC97/SC21/WG4 (along with X3T5.4 in the U.S.) have developed a specification [CMISSP] for a small but powerful set of service elements useful for implementing systems management communication. The specification provides for the following services: Event Notification, Information Transfer, and Control.

Event Notification allows one system to notify another that some "event" of importance to NM has occurred. For example, a Transport connection timing out might be considered an event. The two service elements associated with event notification are Event Report and Confirmed Event Report. Event Report allows an SMAE on one system to report an event to an SMAE on another system. Confirmed Event Report allows a system to report an event and then expect a response back.

Information Transfer, the second service provided by CMIS consists of the single service element: Get. Get is used by an SMAE to request transfer of management information from another SMAE.

The third and most complex service offered by CMIS is Control. Control consists of three service elements: Set, through which an SMAE requests a remote SMAE to set values of attributes within the remote system; Action, through which an SMAE can request a remote SMAE to perform some operation; and Compare, which is used to request a remote SMAE to compare some attribute value with a specified value and then return the result.

CMIS provides a final service element called Blocking which allows combinations of the other service elements to be executed in a coordinated manner on a remote system. Blocking allows complex requests to be performed conditionally and/or atomically at a remote system.

Through the use of just this limited set of CMIS service elements, a wide variety of management communication can be accomplished. CMIS is to be used as the communication basis for the other management facilities such as Configuration or Fault Management.

The Common Management Information Protocol (CMIP) is the protocol used to provide the CMIS services [CMIPSP]. While the details of CMIP are beyond the scope of this report, it is important to note that CMIP uses Connection Oriented Remote Operation Service (CO-ROS) [ROS186,ROS286] as one of its

underlying services. CO-ROS (or just ROS) is itself being modified by ISO, both to relax restrictions that currently do not allow responders as well as initiators to invoke operations, and to allow an alignment between the ISO and CCITT versions of ROS [DROS86].

While CO-ROS is required by the CMIP specification, it is usually desirable to use a Connectionless ROS (CL-ROS) for most LAN operations. CL-ROS would use considerably less network resources since connections (and their related overhead) need not be maintained in the face of the very little traffic that CMIP should normally generate. For example, in the absence of extraordinary conditions, an SMAE may want updated status reports from remote systems only once every half hour. The overhead of maintaining connections to these systems would probably be considerable.

(There are some reports that connection oriented services are more responsive and reliable than connectionless, but there is serious question as to whether these benefits outweigh the resource intensive nature of maintaining connections in the face of infrequent traffic demands that may be expected of network management services.)

Unfortunately, CL-ROS has not yet been defined. In fact, up to now virtually all OSI work has been connection oriented, but this is changing as ISO recognizes the need for connectionless services for a wide variety of applications.

4.3 Configuration and Name Management

One of the management facilities introduced in ISO's Management Framework Document [MGFM86] is Configuration and Name Management. The Framework Document provides a vague but ambitious definition of Configuration Management (CM), but does not discuss Name Management other than to note that distribution of OSI names and relationships to named OSI resources may be assisted by utilization of Directory Service. Therefore, no attempt will be made to deal with the task of discussing Name Management here, rather it will be discussed below under Directory Service.

(Note: The current working paper on Configuration and Name Management [CMSD85] still has no mention nor discussion of Name Management. Apparently, Name Management was added later to Configuration Management - probably because Name Management was (and is) an important issue with no home of its own.)

Configuration Management according to the Framework Document is "the set of facilities which exercise control over, identify, collect data from and provide data to OSI resources for the purpose of assisting in providing for continuous operation of interconnection services. Configuration Management provides facilities to:

a) set the open systems parameters;

b) initialise and closedown OSI resources;

c) collect data giving the open system state both on a routine basis and in recognition of a significant change of state;

d) change the open system configuration."

This definition is rather broad and needs refinement to clarify what activities constitute CM. The working paper on Configuration Management [CMSD85] gives a different, but still broad definition of Configuration Management. This document goes on to give some examples of the types of problems that CM should address such as reading and changing CM parameters, down line loading and enrolling/de-enrolling of systems.

Neither of these documents give a truly concise definition of what CM is or should be. This fact is recognized in the Configuration Management Rapporteur's Report of the September 1986 (Egham) ISO TC97/SC21/WG4 meeting [CMRP86] in which the lack of "any meaningful definition in the current working draft of configuration management" is cited. The CM working group at Egham went on to develop a "Plan for Standardization Work on Configuration Management" [CMSW86] which details the work items that must be accomplished to develop a CM standard. These details include the overall CM model, the abstract syntax and semantics of objects being communicated, and the allowable sequence of activities that may affect resources.

As of the November 1986 X3T5.4 meeting, this model was still being revised as a US contribution to ISO. The other areas of Configuration Management need to be addressed in detail.

TC97/SC21/WG4 has recognized the need to define the scope of Configuration Management [CMRP86] so that it is clear what activities belong in CM versus Fault or Performance Management for example. WG4 also recognizes the need to proceed quickly to resolve these issues, and so ISO held an ad hoc meeting of the CMIS, Security, Fault, and Configuration Management groups in Rome during February, 1987. This is to prepare input to the next WG4 meeting in Tokyo (June 1987).

The General Motors sponsored MAP Network Management activity is now generating a Configuration Management section to its Network Management Specification (MAP/TOP 3.0) to be released in the Spring of 1987. This MAP CM is further along than the comparable ISO specification since it is to be released to implementors soon and also it is limited to MAP (and to a lessor extent, TOP) needs. Specific resource attributes at the layers to be managed and operations on these attributes are identified.

The MAP approach to CM is similar to the ISO's. In fact, their architecture is based on the OSI Management Framework document [MGFM86]. They differ from OSI in that the problems of addition and deletion of resources (e.g., going "offline") are more specifically addressed. (Note: The problem of how to handle addition and deletion of resources and "... the need for specific service elements for creation and deletion of resources .." is mentioned in the Egham CM Rapporteur's Report [CMRP86], which goes on to comment that perhaps CMIS needs to be modified to handle this.)

MAP also differs from OSI in that it considers in greater detail the problems of initialization and termination of resources, i.e., managing systems that are perhaps less than full OSI systems. Examples of such systems include systems that are in the state of needing to be down line loaded or Mini-MAP nodes that include less than the full seven layers. Of course, the MAP specification can offer solutions that deal specifically with problems in the 802.4 factory environment, while OSI solutions must handle more diverse environments, both LAN and WAN.

The ISO view of Configuration Management attributes a great deal more functionality to this facility than does the IEEE 802 view. ISO [MGFM86] and 802 [IESMRL] both consider Configuration Management to be concerned with the initial setup, or subsequent reset, of OSI nodes. However, ISO goes beyond this by including the functionality to manage OSI resources on an ongoing basis. Moreover, ISO suggests the use of Configuration Management facilities as the mechanism by which other management facilities (e.g., Performance Management) can control OSI resources under their purview.

4.4 Directory Service

Directory Service (DS) is to provide, in a user friendly manner, a system to promote communication between users residing on different open systems while isolating these users from the frequent changes of the networks supporting their communication. To do this the DS provides three functions. The first function is a name to attribute(s) binding, i.e., telephone white pages lookup for such information as name to address mapping. The second function is attribute to set-of-name(s) binding, i.e., telephone yellow pages search. The third function is a name to list-of-names binding, i.e., electronic mail lists. All three functions provide a means of ascertaining communications information in order to facilitate interoperability among users/processes residing on different open systems.

The DS is composed of several components. The Directory Information Base (DIB) is the sum of all information contained in the DS. Because of the magnitude of this information, the DIB is usually considered to be a distributed information base. Each segment of the DIB is maintained by and accessed by a Directory System Agent (DSA). Each DSA maintains its portion of the DIB.

communicates with other DSAs to fulfill requests, and receives requests from users via Directory User Agents (DUAs). Each DUA interfaces a user with the DSA and is, thus, responsible for the operation of the communication protocol between the DSA and itself on behalf of the user.

There are two defined protocols in the DS. The first is the Directory System Protocol (DSP) which interfaces DSAs with each other. The second protocol is the Directory Access Protocol which interfaces a DUA to a DSA.

The balloting on DP9594 (the Directory System) closed in February 1987 with the DP overwhelmingly defeated. Due to the results of the vote and the severity of major ballot comments, the entire scope of the standardization effort was changed. Instead of a full functional Directory Systems supporting a complete set of remote facilities (e.g., read, update, delete), the last joint meeting of ISO and CCITT Directory Service experts decided to produce a DS standard which allowed only a remote read capability.

In doing this the group segmented the contents of DP9594 into three categories. The first contains only those items necessary to support a read-only system. The second category contains items which, time permitting, will be included in a 1988 standard. Items in this category include remote modification, access control mechanisms, operational limits (e.g., maximum resources to be expended on an operation), protocol to support the acquisition of knowledge about the DS system itself, protocol support for the replication of information, and the concept of schemas. The third category contains topics which will be deferred until future revision of the DS. Included in this third category are features such as object set descriptors which provide a powerful general purpose filter mechanism for selecting the appropriate entries.

There are currently two international organizations involved in developing DS standards: ISO and CCITT. Early in 1986 they agreed to work together to develop joint standards. Several problems have arisen as a result of this collaboration. The first is that ISO and CCITT are responsive to different needs. CCITT is composed mainly of representatives from member countries' Post, Telegraph, and Telephone authorities (PTTs) and, as such, has a strong telephone bias. ISO is populated by computer equipment manufacturers and users and, as such, represents their interests.

The difference in the intended uses of the DS by the two groups exemplifies the diversity of their needs and interest. CCITT members intend to develop extremely large directories tied together. Some companies supporting ISO intend to develop small directories operating mainly on small machines in a limited environment.

In addition to their different memberships, they work on different schedules. CCITT has a four year study period during which work is developed and presented for adoption at the

conclusion of each study period. The current CCITT study period ends in 1988 with final text due December 1987.

ISO does not conduct business on a fixed time cycle. It employs a multi-stage approach as explained in Section 5.1, "X3T5.4 (OSI Management)".

CCITT is nearing the end of its study period and failure to finish would normally require deferment of a CCITT DS standard until 1992. Most CCITT member bodies want a standard as soon as possible. As was stated above, the DS experts have significantly reduced the scope of the next DP. A second DP ballot will probably begin in July 1987. The results of this ballot will be extremely crucial to the DS standard's progress. Acceptance with only minor comments allow CCITT to issue a recommendation at the end of the current CCITT study period in 1988. (This would require submittal of text by December 1987.) Failure of the second DP or the generation of a significant number of major ballot comments, could present CCITT with a monumental decision as to whether to issue its own standard (by 1988, within the current study period) or to defer to the next study period, resulting in a delay until 1992. If CCITT issues one standard and ISO issues another, interoperability may be seriously threatened.

In the area of security, ISO and CCITT are operating under different guidelines. The ISO Working Group, TC97/SC21/WG4, responsible for DS does not have responsibility for any aspects associated with security. The CCITT Rapporteur's Group on Question 35 (Directory Systems) has a responsibility to develop all aspects of DS including security. The implications of this are not yet clear.

The U.S. is working through two groups to affect the development of the DS standard. The first is X3T5.4. The second is U.S. Study Group D Working Party on Message Handling Services and Directory Systems. X3T5.4 prepares input to ISO and the U.S. Study Group Working Party prepares input to CCITT and specifically Study Group VII Question 35. X3T5.4 and the U.S. Study Group D Working Party have recently developed a unified U.S. position on the DS standard.

4.5 Performance Management

Performance Management (PM) is one of the major facilities of OSI management. According to the Management Framework document [MGFM86], PM provides facilities "to evaluate the behavior of OSI resources and the effectiveness of communication activities". This is accomplished through facilities for the gathering of statistical data and the maintenance and examination of logs of system state information.

As stated in the ISO developed Management Framework document, performance management does not include facilities for control of performance parameters in an OSI system but merely provides for

monitoring of appropriate information to accomplish its objectives. Similarly, in IEEE 802's view [IESMRL] PM gathers statistical data relevant to performance planning and analysis. with the exception that 802 includes in PM the ability to reset counters necessary for the continued operation of a LAN. Thus, Performance Management for both these groups focuses on monitoring rather than on controlling resources. ISO does suggest that the control function for such facilities as PM will be served by the Configuration Management facility. This is unlike the MAP/TOP model [MPNM87], where PM can exercise control.

Performance Management is not scheduled to become a DP until November, 1988 -- one of the last facilities of network management to be addressed by OSI. Therefore, little documentation exists from X3T5.4 or SC21/WG4 defining PM in greater detail. One problem is that clarification is needed as to the boundaries among Configuration, Fault, and Performance Management. This situation was somewhat rectified at WG4's ad hoc meeting held February, 1987 in Rome where the Configuration, Security, and Fault groups met, but Performance did not. (See discussion above in Configuration and Name Management.)

While clarification will certainly help to define PM, its progression is still scheduled to lag other network management facilities within OSI. This is not the case in the MAP planning, where PM along with Configuration and Fault Management are to be progressed most quickly. (Security and Accounting Management are not even considered in the MAP model.)

4.6 Fault Management

Fault Management (FM) provides support for fault detection, fault diagnosis, and fault correction. FM itself uses Common Management services (CMIS/CMIP) for underlying support. The latest working paper on FM management, "Second Working Draft for the Management Information Services Definition -- Part 3: Fault Management" [FMSD86], specifies the following ten facilities for achieving these goals:

1. Spontaneous Error Reporting - This allows one SMAE to send timely error reports to another SMAE.

2. Cumulative Error Gathering - This facility provides for periodic report gathering by one SMAE on behalf of another. It allows for "polling" of error counters on a periodic basis. It also allows for the resetting of error counters.

3. Error Threshold Alarm - This provides for one SMAE to send threshold reports to another. In addition, error thresholds can be set, current settings of thresholds can be determined, and the resetting of those counters to which the thresholds are compared can be reported.

4. Event Logging - This facility allows one SMAE to send all event reports to another SMAE. It provides for the initiation and termination of event logging.

5. Confidence and Diagnostic Testing - This allows for one SMAE to request another SMAE to perform testing on a resource and report back the result. In addition, provision is made for cancelling, suspending, and resuming a suspended test. Finally, it allows for enquiries as to the status of a test procedure.

6. Repair Action Reporting - This facility allows one SMAE to report to another the current status of a resource that has previously been reported as faulty.

7. Trace Communications Path - This facility provides a standard mechanism for cooperating SMAEs to test communications paths and to report results back to the originating SMAE.

8. Resource Reinitialization - This provides for one SMAE to direct another to set a resource to a known initial state.

9. Event Tracing - This facility allows an SMAE on one system to direct an SMAE on another open system to log events locally. It provides for reporting back the collected logs and for stopping the tracing.

10. Fault Management Information Gathering - This provides for further miscellaneous services including dump, statistics, and other related information gathering useful for software and hardware maintenance.

It is recognized that the FM service definition needs further refinement and editing. Although the related protocol document "Fault Management Protocol - First Working Draft" [FMPS86] is a first working draft, has numerous sections omitted, and is expected to need many changes, it does illustrate the procedures needed for Fault Management in OSI. Editing of these two FM documents began at the ISO TC97/SC21/WG4 ad hoc meeting of the CMIS, Security, Fault, and Configuration Management groups in Rome during February, 1987.

4.7 Security Management

Security is an unusual aspect of communications. Its goals may seem to contradict with the goals of Open System Interconnection, since security usually implies maintaining a "closed" system in some sense. However, security is both possible and necessary in open systems. Before proceeding with a discussion of Security Management, it is important to understand what is meant by OSI security. A brief explanation is given here, but for a more complete overview see "Considerations for Security in the OSI Architecture" [BRAN86].

4.7.1 OSI Security

Security is an area often surrounded with a "mystique" of misunderstanding, and there is often an apparent unwillingness by those people most familiar with the problems and solutions for providing and insuring security (for reasons that may be perfectly reasonable) to discuss or publish information about it. Yet, to provide secure open systems, the problems must be aired and proposed solutions presented. Many groups within the ISO standards making community are now doing just that.

Probably the most significant is the architectural work on security by ISO TC97/SC21/WG1 which has lead to a document [DAD286] entitled "Proposed Draft Addendum 2 to ISO 7498 on Security Architecture". This document, which has recently become a Draft Addendum, is currently being revised to include numerous changes suggested in its balloting. It describes the concepts and goals of OSI security. A complete discussion of all aspects of OSI Security Architecture is beyond the scope of this report. However, a brief description is necessary before proceeding to discuss Security Management.

While there are many aspects to computer data security, it should be noted (as stated in the Architecture document) that "OSI security functions are concerned only with those visible aspects of a communications path which permit end systems to achieve the secure transfer of information between them". Thus aspects of security unrelated to OSI information transfer (e.g., physical site security) are beyond the scope of OSI security.

The Architecture proposes a set of services, a set of mechanisms for achieving them, and a suggested list of layers where these mechanisms could be employed to produce the desired security features. To understand OSI Security it is important to understand the services to be provided.

The five major security services specified in the Draft Addendum are authentication, access control, confidentiality, integrity, and non-repudiation. Several of these are specified at various granularities and the following list of specific security services are defined in the document:

1. Data Origin Authentication: The corroboration that the source of data received is as claimed.

2. Peer Entity Authentication: The corroboration that a peer entity in an association is the one claimed.

3. Access Control: The ability to restrict access to a resource.

4. Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. Confidentiality is to be applied on a connection basis, a connectionless basis (to an individual

message), or on a selective field basis.

5. Traffic Flow Security: A confidentiality service to protect against traffic analysis.

6. Connection Integrity with or without Recovery: Integrity of all user data on a connection with or without attempted recovery. In addition, detection of any modification, insertion, deletion or replay of any data is provided. Integrity is defined as the property that data have not been altered or destroyed in an unauthorized manner.

7. Selective Field Connection Integrity: Integrity of selected fields within a message which is to be transmitted.

8. Connectionless and Selective Field Connectionless Integrity: Similar to Connection oriented integrity, but applied on the basis of individual messages.

9. Non-repudiation, Origin: Proof of the origin of the data provided to the recipient of data which will protect against any attempt by the sender to deny falsely sending the data or its contents.

10. Non-repudiation, Delivery: Proof of the delivery of data provided to the sender such that the recipient cannot later deny receiving the data or its contents.

This list is too long to comment on in detail. Certain services such as integrity, access control, and confidentiality are probably very important to a broad class of OSI users. Non-repudiation is often not so important, but, of course, to the banking community, it is of utmost importance.

While there are many mechanisms proposed for achieving security, probably the most important is encipherment (also known as encryption). As the Security Addendum notes "encipherment provides confidentiality and assistance towards data integrity". It is also needed to assist in providing the other services required for security.

A substantial amount of work has been done at the NBS to produce the Data Encryption Standard (DES). This is known internationally as Data Encryption Algorithm - 1 (DEA-1). It has been proposed as an International Standard but the appropriateness of adopting cryptographic algorithms as International Standards has been questioned within ISO. It is uncertain whether it will become an IS. At last report its status was under review by ISO TC 97's legal office.

An important advance in the science of encipherment is commonly known as public key algorithms. For DES, both the originator and the recipient must use the same secret key to

encipher and decipher messages. For public key algorithms, an associated pair of keys is used. One is made public and the other is held secret. One key enciphers and the other deciphers. This property can be used in several ways for assisting in providing OSI security.

An important use is for proving authenticity. A user publishes a public key for the use by potential recipients of messages of secure messages. When the user sends a message, the recipient attempts to decipher it with the published public key of the sender. If the message deciphers correctly, the recipient "knows" that it must have been sent by the authentic originator since only that person knows the correct matching secret key used to encipher the message. The publication process requires integrity such that one public key cannot be substituted for another.

ISO TC97/SC20 is the group responsible for developing data encipherment standards. It is investigating DEA-1, public key algorithms (e.g., the RSA algorithm), modes of operation for encipherment, registration of enciphering algorithms (for providing families of such algorithms), and some other aspects of cryptographically-based security.

ISO TC68 (Banking) has a subcommittee (SC2) concerned with Electronic Funds Transfer (EFT). Its work on data integrity, key management, and encryption may have a great impact on emerging OSI security standards.

4.7.2 Security Management Architecture

Security Management (SM) is the management (monitoring and control) of the OSI security facilities that are installed or required to be installed to achieve desired security services. To accomplish this, the Management Framework document [MGFM86] calls for features to be provided for: authorization facilities, access controls, encryption and key management, authentication, as well as maintenance and examination of security logs.

To support development and further refinement of these features, a document was produced at the TC97/SC21/WG4 meeting at Egham in September, 1986. This is the "Proposed Draft for Management Information Services Definition, Part 7, Security Management Definition" [SMSD86]. This document introduces a set of facilities for SM. Some of the concepts are fairly well developed and others are to be determined later. As it states itself, further editing is required. However, a discussion of some of its proposals is worthwhile to gain insight into the future direction of SM.

The document divides SM functions into four broad categories as follows:

Authentication Management - This involves management activities, such as distribution of passwords and keys, in support of authentication. It may involve maintenance of authentication attributes. Also, it may involve a protocol for communicating authentication information.

Access Control Management - This involves the maintenance of access control lists and may include password distribution as well as a protocol for communications of maintenance information.

Key Management - This is the maintenance of keys used for encipherment, including their generation, storage, distribution, etc. Some functions will be performed outside of the OSI environment, including the physical distribution of keys by trusted means. A protocol between communication entities may be involved.

Security Audit Trails and Event Handling - This includes the remote collection of audit records as well as enabling and disabling of logging.

The document goes on to describe SM services in more detail as well as service primitives used. Also, the service elements associated with each primative are described. The document is an excellent first draft to serve as a basis for continued refinement of the Security Management efforts.

However, before SM can be employed, the security features developed in the Security Architecture Addendum [DAD286] must be refined and implemented. Without these features, Security Management is useless.

The difference between ISO's [MGFM86] and IEEE 802's [IESMRL] approach to Security Management is in the comprehensiveness of the facility. Both groups include access control management as part of Security Management. Access control encompasses monitoring and allowing or denying access to the LAN itself or to management information obtained from stations on the LANs. However, while 802 encompasses only this limited functionality, ISO includes four additional areas of functionality including authorization facilities, key management for encryption, authentication, and maintenance and examination of security logs.

4.7.3 LAN Security Problem

Probably the most important problem in the security area that needs to be solved soon is the issue of data confidentiality in the LAN environment. (And data confidentiality problems soon contribute to problems in data integrity, authentication, access control, and other areas.) Most LANs operate in a broadcast mode. All messages pass all stations in the LAN. Without encipherment, it is possible for any station to monitor the traffic to and from all other stations. This is a serious problem and it may be years

before interoperable, commercially available, products are available to solve it.

(Note: There are rumored to be encipherment products under development that may be placed in transceivers. However, it is not known when these will be commercially available. In addition, to provide for data confidentiality between pairs of stations on the LAN, the encipherment must be provided on the basis of a unique characteristic of the traffic between the stations, such as the source and destination addresses contained in the packets transferred. These rumored products are expected to contain this pairwise encipherment capability. However, for even moderately sized LANs the number of station pairs create a major key distribution problem.)

For the interim it is important to maintain physical security for all LAN segments to prevent an intruder from "tapping" the line. Further, the stations on the LAN must be trusted, and so must their (human) management. Even then security problems can arise, such as when visiting service personnel appear to monitor the lines in order to diagnose problems. (Such line monitoring (and associated data recording) are the most common method of diagnosing problems with LANs.)

4.8 Management Information Base (MIB) and Structure of Management Information (SMI)

The Management Framework document [MGFM86] introduces the notion of a Management Information Base (MIB), a conceptual repository of all OSI management data in an OSI environment. This concept is introduced but not expanded. However, the document notes that no particular form of storage is implied, i.e., it is an implementation matter.

A great deal of interest has been generated lately in refining the concept of the MIB. This refinement includes expansion into a related area entitled Structure of Management Information (SMI). Once the conceptual SMI has been determined, this information can be presented to the layer development groups for resource object identification.

The first ad hoc meeting of the ISO TC97/SC21/WG4 SMI group took place in Rome in February, 1987. At that meeting the scope of SMI was stated as including the following topics:

defining types of management information and the relationship between these types;

defining the protocol operations that can be performed upon management information;

discussing the naming and identification of management information.

One of the biggest problems in defining the SMI is the terminology to be used. For example, at various times, the terms "resource", "resource attribute", "management information item", "management object", as well as others have been used to describe the objects being managed. Various groups have different connotations associated with the different terms -- so confusion is common. It will be a major advance in SMI definition if the WG4 meeting in Tokyo, June 1987 can devise stable and useful terminology.

A promising new concept is the separation of descriptors of managed information objects from the objects themselves. This concept, recently developed by X3T5.4 in the U.S., is to be presented to ISO at the WG4 June 1987 meeting. Separating descriptors from the managed objects appears to allow for accurate modeling of the resource management problems within layered open systems. Further development should lead to improved SMI modeling.

While the work on SMI is relatively immature, the importance of this work cannot be underestimated. Without it, resource identification and specification of allowed operations on resources cannot proceed quickly. Such a delay would impede the overall implementation of OSI network management.

4.9 Accounting Management

Accounting Management is "the set of facilities which enable charges to be set for the use of resources and costs to be identified for the use of those resources."[MGFM86] While this is certainly important for wide area networks which usually tariff resources, it may not be of such importance to local area network users. Since LAN management is of primary importance to the sponsors of this report, and since Accounting Management is the least mature of the SMISs (i.e., there are few recent working papers dealing with it and it is scheduled to be reach IS status relatively late), it will not be discussed further.

5 OSI Network Management Standards Making Groups

This is a description of the major management standards making groups that were surveyed to provide input to this report. It is by no means complete. The first body to be discussed is X3T5.4, the primary OSI management standards making body in the United States. The progress of other related standards making bodies will then be compared to X3T5.4.

There are several groups producing standards for OSI network management. Primary among these are the International Organization for Standardization (ISO), the American National Standards Institute (ANSI), the Institute for Electrical and Electronic Engineers (IEEE), The International Telegraph and Telephone Consultative Committee (CCITT), and the European Computer Manufacturers Association (ECMA). Most of these are

further subdivided into subgroups to address the various aspects of network management.

Limitations of time and resources dictate that the list of groups surveyed be incomplete. However, an attempt has been made to focus on the most representative bodies and those with the greatest influence upon producing the final standards.

5.1 X3T5.4 (OSI Management)

While there are many groups participating in OSI management standardization (e.g., IEEE 802.1, and ANSI's ASC X3S3.3), the primary responsibility for developing OSI management standards in the United States rests with ASC X3T5.4.

X3T5.4 presents its technical input to its parent committee, X3T5. X3T5 in turn approves (or in rare cases disapproves) X3T5.4's position for submission to ISO. With X3T5's approval, members of X3T5.4 represent the U.S. at meetings of ISO's Technical Committee 97, Sub Committee 21, Working Group 4,

ISO's process for developing standards involves a multi-stage (usually referred to as ISO TC97/SC21/WG4.) approach. The four stages in the development cycle are: working paper, Draft Proposal (DP), Draft International Standard (DIS), and International Standard (IS). During the first stage a working paper is developed. When the working paper matures to the point that it contains well developed technical concepts, it is registered as a DP. Registration is either by a vote at a meeting of the appropriate ISO subcommittee (TC97/SC21 for most OSI management related standards development work), or by letter ballot of the member bodies. After registration the DP is distributed for a 90 day ballot. Multiple ballots, each followed by an editing meeting, may be required. Successful passage advances the DP to the DIS level. As a DIS, the document is usually considered sufficiently technically stable to serve as the basis of initial implementations.

Once at the DIS level, the document is distributed for a 180 day ballot. As with a DP, a DIS may require multiple ballots/editing meetings. A successful ballot elevates the DIS to the level of IS and completes ISO's process.

In either of the ballots listed above "no" votes from member bodies must be accompanied by the reason(s) for the vote. Proposed text changes are often included with the votes. Input from all member bodies is considered. "No" votes from participating member countries is especially critical in the balloting, and their proposed changes must be carefully considered. Usually unanimous agreement must be reached before a document can progress to International Standard. Therefore, a single "no" vote from a participating member country usually requires reballoting after consensus is reached on the proposed changes.

In the interest of generating a single OSI management structure to avoid duplication of effort and to allow for world wide interoperability, X3T5.4 is cooperating fully with TC97/SC21/WG4 to develop network management standards. It is significant to note that X3T5.4 reviewed the latest documents submitted as Draft Proposals (DPs) at the September, 1986 ISO meeting held in Egham, England, and made significant comment on them. The comments were so negative that X3T5, X3T5.4's parent committee, recommended that the US vote "No" on each of them. With negative votes from the US and several other major countries, each of these tentative DPs (identified below in Status of Documents) was defeated and must now be revised and sent out for a second ballot.

Until very recently X3T5.4 was split up into three working subgroups. One was concerned with the OSI Management Framework (an Architecture or model); one primarily with CMIS and CMIP; and one with Directory Service.

At the most recent meetings further subgroups were established to deal with Security Management, Fault Management, and Configuration Management. These subgroups are preparing input for the June 1987 meeting of ISO TC97/SC21/WG4 in Tokyo. Draft Proposals in each of these three areas are scheduled [SC21RP] to be registered by February 1988.

5.1.1 Status of Documents

5.1.1.1 Management Framework

[MGFM86] "Management Framework Addendum" (to the OSI Basic Reference Model) This document was a Draft Proposal defeated in the ballot that closed February 12, 1987. It will be revised and probably be resubmitted for balloting after the June 1987 ISO TC97/SC21/WG4 meeting in Tokyo.

5.1.1.2 CMIS/CMIP

There are four major documents concerned with CMIS and CMIP. Since there were so many significant changes to them suggested by X3T5.4, the U.S. voted "no" on each. These documents were Draft Proposals defeated in the ballot that closed February 12, 1987. They will be revised and probably be resubmitted for balloting after the June 1987 ISO TC97/SC21/WG4 in Tokyo.

[CMISOV] "Management Information Service Definition - Overview"

[CMISSP] "Management Information Service Definition"

[CMIPOV] "Management Information Protocol Specification - Overview"

[CMIPSP] "Management Information Protocol Specification"

5.1.1.3 Directory Service

[DIRSER] "The Directory" This document was rejected as first DP. A revision of the document should be produced at the next collaborative meeting of ISO and CCITT in Tokyo, June 2-10, 1987. A second DP ballot is expected to begin in the July - August 1987 timeframe.

[DIRSEC]"Directory Systems: Authentication Framework" This document is currently being progressed by CCITT. A separate effort is underway by ISO SC21/WG6. Alignment of these two efforts should occur at the final 1987 collaborative CCITT/ISO meeting in November. differences.

5.1.1.4 Other Documents

The documents cited here have not yet achieved Draft Proposal status: however, they are significant in that they show the direction of future work within X3T5.4. They are not broken out by subgroup because X3T5.4 may reorganize its subgroups in the future to progress them once the management framework and common management issues have stabilized.

[FMSD86] "Second Working Draft for the Management Information Services Definition -- Part 3: Fault Management" This document specifies the facilities of Fault Management. It was edited at the ISO TC97/SC21/WG4 Rome ad hoc meeting in February, 1987.

[FMPS86] "Fault Management Protocol - First Working Draft" This document specifies the protocol mechanisms used to provide Fault Management service. Since this is a first working draft, numerous sections are omitted, and many changes can be expected, but it illustrates the procedures needed for Fault Management in OSI. It was edited at the ISO TC97/SC21/WG4 Rome ad hoc meeting in February, 1987.

[CMRP86] "OSI Management Information Services - Configuration Management Rapporteur's Report: Egham 9-11 September 1986" This document summarizes the discussion at the Configuration Management sub group meeting at Egham; presents the proposed output document ([CMSW86]); and presents proposed recommendations. The most important aspect of this document is probably the last -- a recommendation for a planning meeting soon to develop a better model for SMIS management in order to progress CM to DP by February, 1988.

[CMSD85] "Information Processing - Open System Interconnection - Management Information Service Definition - Part 5: Configuration Management Service Definition" This is a document that was produced at the ISO TC97/SC21/WG4 meeting at Philadelphia in November, 1985. It introduces some ideas about CM, but is more of an initial outline than a definition. This document is probably obsolete.

[CMSW86] "Plan for Standardization Work on Configuration Management" This document was produced by the CM subgroup at Egham. It introduces some concepts about the states of resources to be managed. However, it was apparent from recent X3T5.4 Meetings, that these concepts need further refinement or revision. (Further working papers concerning Configuration Management were developed by X3T5.4 for submission to the June 1987 WG4 meeting in Tokyo. However, pending final editing they are not yet available for distribution.)

5.2 IEEE 802 (Local and Metropolitan Area Networks)

The 802 project of the IEEE is chartered to develop a family of standards for local area networks (LANs) and metropolitan area networks (MANs). The reference model used by IEEE 802 is patterned after the OSI Basic Reference Model [IS7498]. The 802 standards relate to the full functionality of the lowest two layers of the OSI Basic Reference Model as well as to the functionality of the higher layers regarding interworking of network and systems management. Figure 4 (from [IEOISM]) demonstrates the relationship between the OSI and IEEE reference models and indicates where the 802 standards are designed to detail the workings of the OSI Reference Model. (The layer labeled "internetwork" in Figure 4 refers to the internet sublayer of the network layer. The function of this sublayer is to enable communication between hosts on different networks.) Figure 5 (from [IEOISM]) shows how work on this family of standards has been divided among several working groups and how these standards are related.

The work in protocol management under IEEE 802 falls into two basic categories--systems management and layer management. This represents a parallel treatment to that of ISO. The work in 802.1 focuses primarily on delineating the overall function of systems management. The proposed systems management trial use standard [IESMRL] specifies both the common set of services for managing system resources and the common portion of the protocol for providing the specified services. This provides the overall framework by which an OSI system can be managed. However, it is incomplete without, at least, the second part of the standard which is the layer or resource specific systems management standards. The development of these layer specific standards has been delegated to each of the relevant subcommittees as represented in Figure 6 (from [IELSSM]). The specific systems

management sections of each of these layer standards specify 1) the resources of the layer to be managed, 2) the system management information and services specific to the resources, and 3) the resource-specific portions of the systems management protocol by which these services and information are accessed.

Systems management is able to use the layer management services which are provided by the MAC and physical layer Layer Management Entities (LMEs) by using the Layer Management Interface (LMI). By so doing, systems management is able to 1) manipulate management objects within designated layers, 2) initiate actions within the layers, and 3) receive notification of significant layer detected events.

In addition to the two major architectural entities involved in systems management described by ISO (i.e., the Systems Management Application Process, SMAP, and the Layer Management Entity, LME), IEEE 802 adds a third component, the "Mapper". The addition of this entity illustrates the following area of divergence between ISO and IEEE 802.

ISO is proposing that systems management can only function when operating on a full stack of OSI protocols (i.e., all seven layers). Anything less than a full stack of OSI protocols does not provide sufficient functionality to support systems management. However, IEEE 802 allows less than full seven-layer OSI end systems (e.g., as in various types of bridges). As a consequence, IEEE 802 has proposed the Mapper entity to take up the "slack" on these systems and to provide the missing functionality associated with the missing OSI layers. Although the Mapper is not specified in detail, there is a description of how, in general, it is to function. The Mapper operates on less-than-full-stack OSI end systems and is responsible for "transporting systems management data provided by a user". It is designated a Mapper because its primary service is to map the "communications service required by the user to that provided by an incomplete end-system in a station".

5.2.1 Status of Documents

5.2.1.1 Systems Management

At the IEEE 802 meeting in San Diego on November 17, 1986, the ballot results were reported for the following three primary documents dealing with systems management.

[IEOISM] "Draft IEEE 802.1 Standard: Part A, Overview, Interworking, and Systems Management", Draft D

[IESMRL] "Draft IEEE 802.1 Standard: Part B, Systems Management", Revision L

[IESLPA] "Draft IEEE 802.1 Standard: Part B--Systems Management, System Load Protocol", Revision A

All three ballots failed. A probable reason for these ballot failures was a lack of sufficient interest in these documents because of an anticipation that the comparable ISO documents will eventually be adopted. It was felt, however, that the great amount of work having gone into their development should not be wasted and the knowledge to be gained from some use of them could be helpful to the entire systems management effort. Therefore, the decision was reached to make these documents Trial Use Standards. The rationale for this decision appeared to be that convergence with ISO is desirable and the ISO documents, particularly CMIP and CMIS, will gain overwhelming approval when ready. Therefore, in the interim, before the ISO documents become fully developed and adopted as standards, these three 802 documents will be used as guidance, and feedback will be offered through liaison reports to ISO. The ultimate outcome will probably be to migrate to the ISO standard.

5.2.1.2 Layer Management and MAC Bridge Standard

On a bridged LAN, composed of two or more separate LAN segments (either of the same or different types), a Medium Access Control (MAC) Bridge may be used to interconnect these separate LANs by relaying frames between the separate MAC layers of the bridged LANs (see Figure 7). The MAC Bridge differs from the commonly referenced link level bridge in that, for the MAC bridge, there is no common logical link control (LLC) procedure in the bridge above the MAC layers [IEMCBA]. With regard to whether a common approach or a MAC specific approach should be taken to systems management, a resolution was proposed and consensus reached at the November, 1986 meeting that a combination of the two approaches is the way to proceed. More specifically, 802.1 will develop a MAC bridge standard to be operable with all 802 compatible MACs. In addition, each MAC working group may develop additional MAC bridge standards specific to its own MAC. Any such new MAC standard must incorporate mechanisms which allow it to interoperate at the MAC Sublayer with the basic standard.

One possible difficulty which may develop, despite this resolution, concerns the proper method of achieving routing. The 802.1 subcommittee, which has overall responsibility for 802 LAN internetworking standards, had been supporting transparent bridge routing for internetworking by use of a spanning tree algorithm [SPNTRE]. However, the 802.5 subcommittee is being urged by certain members (primarily those from IBM) to use a source-routing internetworking method and 802.1 appears to be permitting 802.5 to pursue this course. Some 802 members consider this to be a possible overstepping of the 802.5 subcommittee's jurisdiction in an attempt to make an end-run around the previously agreed upon position.

Figure 8 illustrates the three different service interfaces operative in systems management. The Systems Management Interface (SMI) is the "service interface for systems management services provided by (the SMAE portion of) SMAPs. The SMI is used to 1) initiate management operations and receive their results, and 2) receive unsolicited reports of events". The second interface is the Systems Management Data Service Interface (SMDSI) which is the "service interface for the exchange of protocol data units". The SMDSI is "used to 1) send systems management protocol data units (SM_PDUs) to remote SMAPs and 2) receive incoming SM_PDUs from remote SMAPs". The last interface is the Layer Management Interface (LMI).

Since it is only at a layer, rather than the system level, that specific management readings or settings can be made, systems management requests must be mapped onto one or more layer management activities. Layer Management (LM) is that activity which takes place across the LMI at the Nth layer. The LMI is "used to 1) make management requests of the particular layer and 2) receive notification of an event within a particular layer". "The LMI is the service interface provided by LMEs. The precise nature of the LMI depends on the layer being managed and is therefore specified in the layer specification. However, in order to structure the SMAP and to simplify and harmonize implementations, a set of generic interface primitives" is specified in the systems management specification [IESMRL] and also used in the layer management specifications ([IELM23], [IELMDB], [IELMDD], [IELSSM], [IEMANB], [IEMCBA], [IEMLM7], and [IEPLM3]).

Service primitives are invoked either in response to a request from the Systems Management Entity on the same station or as a consequence of a request from a peer layer management entity (LME) on some other station. The five basic management operations (LM_SET_VALUE, LM_COMPARE_AND_SET_VALUE, LM_GET_VALUE, LM_ACTION, and LM_EVENT) are used to observe and manipulate objects within a Layer Management Entity. Layer Management Entities are entities within a layer which contain management parameters, actions and events. Figure 9 illustrates the existence and use of three different types of layer management entities at the LLC sublayer. In IEEE 802's basic systems management document [IESMRL], an object is defined as "either a Parameter or an action-object". A Parameter is further defined as a "set or series of one or more individual parameters which can only be accessed as an atomic set, and not individually". An individual parameter, moreover, is a "single defined parameter within an LME whose value can be read and/or changed by an SM_user". Finally, an action-object is "a state transition or sequence of actions within an entity.

These definitions and their implications for the types of items managed contrast somewhat with what ISO conceives of as resources. Although ISO's definition of manageable resources is not well-defined, one interpretation of ISO's concept is that a management resource comprises an entire layer, such as Transport,

and the "attributes" of the resource refer to the parameters within the layer. (Note: The concept of resources and the relationships between resources is currently under review by ASC X3T5.4 and ISO TC97/SC21/WG4.) There is a fundamental difference between these two concepts and the smaller granularity of objects in the 802 concept seems to have allowed 802 to make considerably greater progress in defining the LM, even to the point of specifying the particular objects to be manipulated at the different layers.

The following is a list of documents relevant to layer management and MAC bridges with indications as to the status of work within these groups as of the November, 1986 meeting.

[IELM23] "Revised Draft Copy: Layer Management Proposal for 802.2 Section 2.3"
The 802.2 LLC sublayer management document is ready for its first working group (WG) letter ballot. Additional work was done on this document at an interim meeting in January, 1987.

[IELMDD] "IEEE P802.3-86/0.05D: Layer Management"
Draft E is now under review and being circulated for comment with additions of Pascal planned to bring it to Draft F.

[IEMLM7] "IEEE Draft Standard 802.4 Revision: Section 3: MAC Layer Management, Revision 7"

[IEPLM3] "IEEE Draft Standard 802.4 Revision: Section 9: Physical Layer Management, Revision 3"
The 802.4 MAC and Physical layer management documents are currently being edited and revised in order to be ready for the March, 1987 IEEE 802 meeting in New Orleans so that they can be incorporated into the Draft G ballot which will close in July of 1987 at Vancouver. Draft G is expected to be compatible (almost) with the anticipated IS from ISO.

[IELMDB] "IEEE 802.5 Layer Management, Draft B"
Coordination between 802.5 and 802.1 is being sought and 802.5 also considers it important at this time to work on identifying appropriate work items. The issue of the appropriate routing algorithm, mentioned above, is coming to the foreground, with 802.5 desiring its own source routing scheme.

[IEMANB] "Draft IEEE Standard 802.6 Metropolitan Area Network (MAN) Station Management"
Perhaps as a consequence of the very formative nature of 802.6, there is little concern for station management currently. Many of the concerns and issues dealt with by 802.6 fall into the category of political issues rather than technical ones. A re-evaluation of the

scope and focus of 802.6 was considered appropriate.

6 Other Activities and Standards Making Groups

6.1 X3T5.1

Accredited Standards Committee X3T5.1 is tasked by ANSI with developing standards in the U.S. related to OSI architecture. It is the U.S. counterpart to the ISO TC97/SC21/WG1 group, which also works on OSI architectural issues. X3T5.1's influence on Network Management development occur mainly in two areas.

The first is in questions of jurisdiction. When one group cannot decide whether or not the solution to a certain problem is within its area, X3T5.1 may be able to resolve the issue on the basis of OSI architecture. Thus it often resolves possible "turf battles" between groups.

The second area of influence is Security Management. X3T5.1 has participated in the development of the "Proposed Draft Addendum 2 to ISO 7498" [DAD286], discussed above in Security Management. This is a major contribution to OSI architectural development work.

6.2 GM Manufacturing Automation Protocol (MAP) Group

General Motors Corporation took an early lead in the acceptance of OSI protocols by adopting OSI as the communications basis for their major project to develop the fully automated factory. GM developed a Manufacturing Automation Protocol (MAP) in the early 1980's in order to assure interoperability of products from different vendors. This was prompted by the adverse experience of seeing artificial "islands of automation" develop in the factory environment because products from different vendors did not interoperate.

The first major public demonstration of multivendor interoperability using OSI based protocols took place at the June 1984 National Computer Conference (NCC), with General Motors as a leading sponsor of this demonstration. The term "MAP" is now associated with the entire GM factory automation communications effort, not just that portion concerned solely with the Application layer. MAP specifies standards for all seven layers. Other companies have joined with GM to progress MAP standardization, both manufacturers (users of factory automation products) and vendors of automation products.

A related set of standards, entitled Technical Office Protocol (TOP) is being jointly developed for office automation. The TOP effort is led by Boeing. Whereas MAP is primarily based on products using IEEE 802.4 Token Bus LAN technology, TOP is based more on IEEE 802.3 CSMA/CD LAN and X.25 WAN technology. These diverse technologies can be interconnected through gateways and commonality of design can be achieved at the intermediate

layers (e.g., Transport and Network).

The current MAP specification, Version 2.1, is enjoying moderate success. Factory automation products built to the 2.1 specification are now available. However, one of the major problems with Version 2.1 is its inadequate network management facilities.

A new version of the MAP specification (Version 3.0) is almost completed and is to be released in the Spring of 1987. (This version is being developed jointly with the TOP specification. However, the major design concerns tend to be oriented toward MAP rather than TOP. As more products become available for office automation, it would not be surprising for the TOP effort to eventually surpass MAP. But for now, at least, it seems that MAP is leading the way.)

Network management is a major part of the MAP/TOP 3.0 specification. It is based upon OSI network management principles. However, since the OSI network management standards are clearly not complete and GM is anxious to have Version 3.0 products available for the June 1988 demonstration, the MAP/TOP network management specification uses ad hoc techniques where the ISO specifications are not yet available. Furthermore, MAP/TOP has identified those resources and attributes to be managed, something that ISO has yet to do. Therefore, the resource identification eventually developed by ISO will likely differ from that used by MAP/TOP.

MAP/TOP 3.0 network management contains three management facilities (functional areas): Configuration Management, Performance Management, and Fault Management. These three areas are also addressed by ISO in its Management Framework document [MGFM86]. The ISO document addresses two additional areas: Security Management and Accounting Management. MAP/TOP has placed a different set of priorities on these areas than has ISO. While the ISO progression for standardization emphasizes Security Management as well as Configuration and Fault, it is not initially as concerned with Performance Management.

The emergence of the MAP/TOP 3.0 Network Management Requirements Specification may cause a major problem in Network Management development. Since 3.0 will be available very soon, vendors must make a choice between implementing it, or waiting several years until ISO network management standards are stable enough to implement products for delivery. For those vendors who choose to produce 3.0 products, it will be difficult to then develop newer, probably incompatible products based on the ISO standards. Those vendors who choose not to develop 3.0 products may be eager to deliver ISO conformant products. It is possible that a divergence of network management products could occur. Since MAP is publicly committed to the adoption of International Standards, eventually the two sets of standards will most certainly merge. However, there may be an incompatible set of

Version 3.0 products still being used long after the merger. (A more positive aspect of this potential problem is that early experience with 3.0 Network Management may indicate interoperability problems that will lead to better ISO standards and products.)

6.3 NBS OSI Implementors Workshop

The NBS/OSI Workshop Series for Implementors of OSI Protocols (more commonly referred to as the NBS OSI Implementors Workshop) meets five times per year in the Washington, DC area. The workshop series was organized in 1983 "to bring together future users and potential suppliers of OSI protocols. The workshop accepts as input the specifications of emerging standards for protocols and produces as output agreements on the implementation and testing particulars of these protocols. The process is expected to expedite the development of OSI protocols and promote interoperability of independently manufactured data communications equipment."

The Workshop has contributed extensively to demonstrations of the interoperability of systems supplied by many major vendors using OSI protocols. These demonstrations include the 1984 National Computer Conference (NCC) and the 1985 Autofact Conference.

The workshop currently supports nine Special Interest Groups (SIGs). These are:
File Transfer, Access, and Management (FTAM),
X.400 (Message Handling),
Lower Layers,
Performance,
OSI Security,
Directory Services,
Virtual Terminal,
Upper Layers, and
Office Document Architecture (ODA) and Office Document Interchange Format (ODIF).

The participants of the Workshop spend most of their time discussing technical issues in the SIGs. There, proposals for contributions to the overall implementors' agreements are developed. These proposals are then voted upon by the entire Workshop in plenary.

Although there is no Network Management SIG, the Performance, Security, and Directory Services SIGs address these aspects of Network Management. Recently support has appeared for organizing a Network Management SIG. The establishment of a NM SIG is scheduled to be discussed and voted upon at the May 1987 meeting. Based upon tentative support expressed at the March meeting, the establishment a NM SIG in May is likely.

The NBS Workshop has contributed greatly to the progress of OSI implementations by developing these agreements which allow vendors to cooperatively test their emerging products and by encouraging users that OSI "really works" as demonstrated at major trade shows. The agreements often clarify ambiguities in developing standards and propose methods for interoperating before implementations of supporting standards are complete. For example, the 1984 NCC demonstration consisted of a subset of FTAM operating directly over Transport. (There were no Presentation nor Session implementations available then.)

6.4 X3S3.3

X3S3.3 is the ANSI group developing standards for Layers 3 and 4 (Network and Transport) of the OSI Reference Model. The current work spans many areas but the most important with regard to Network Management are its work on Layer Management for Layers 3 and 4, and its work on Intermediate System to Intermediate System (IS-IS) Framework Architecture Document [S33F86]. (IS to IS protocols, explained below, are very important to solving network routing problems.)

To provide for layer management of Layers 3 and 4, X3S3.3 is collaborating with the X3T5.4 and IEEE 802 committees that are working on Network Management standards. X3S3.3 is compiling lists of resources and their attributes to be managed at each of these layers. An initial draft of these lists was produced at the January, 1987 X3S3.3 meeting. This list will require considerable further refinement.

The Framework Document [S33F86] is an architectural model of how routing should be accomplished in an ISO environment. The model is a precondition to the development of an IS-IS protocol which will specify the type of information exchanges to be performed so that each and every IS will have usable up-to-date information to be used for routing purposes.

6.5 The Corporation for Open Systems (COS)

The Corporation for Open Systems (COS), organized in 1986, is a consortium of approximately sixty member companies (primarily vendors) who pay annual dues to participate in COS activities. The stated objective of COS is:

> "... to provide a vehicle for the acceleration of the introduction of interoperable, multi-vendor products and services operating under agreed-to OSI, ISDN and related international standards to assure wide-spread customer acceptance of an open network architecture in world markets." [COSP86]

One of COS' primary activities is the development of conformance testing and certification methodology for OSI systems. There have been some problems in this area. In fact, it was COS's delay in the procurement of conformance testing systems that

caused the planned demonstration of the MAP 3.0 protocol suite at the Autofact 87 conference to be cancelled. (It has been rescheduled for Baltimore in June of 1988.)

Other activities of COS include the coordination of member companies efforts in OSI standards development. Due to the heavy representation of vendors within the COS membership, its influence on the standardization efforts is likely to reflect the views of the vendors. It has been reported that two user organizations have considered withdrawing from COS membership.

Recently, there has been an effort by COS to recruit more user members including offers of a reduced membership fee. Whether this effort will be successful, and what effect it has on COS, remains to be seen.

6.6 The Government OSI Procurement (GOSIP) Specification

The Government OSI Procurement (GOSIP) Specification specifies Federal Government procurement policy with regard to OSI. [GOSI86] It is expected to become a Federal Information Processing Standard (FIPS). It will become the standard for all Federal agencies to use when procuring ADP systems or services and communication systems or services. GOSIP will be mandatory for purchases of minis or mainframes that provide functionality equivalent to the protocols defined in GOSIP. Thus, for example, if an agency is purchasing a message handling system, and since a message handling system is specified in GOSIP, it is mandatory to purchase a GOSIP compatible system. On the other hand, since teleconferencing is not specified in GOSIP, an agency requiring such a service is not required to consider GOSIP in its procurement specfication.

A draft copy of the GOSIP specification dated Dec. 18, 1986 has been distributed for comment. The comment period ended March 13, 1987, and the results are not yet available.

GOSIP requirements are based on three levels of sources:
Primary: NBS/OSI Implementor's Workshop Agreements. (MAP 2.1 specifications incorporated earlier versions of these Agreements.)
Secondary: ISO ISs and CCITT Recommendations, DISs, DPs, and working papers.
Tertiary: DOD Management standards. (GOSIP notes missing OSI management standards.)

The current GOSIP draft specifies two Application layer protocols. The first is File Transfer, Access, and Management (FTAM), with additional document types beyond those specified by the Workshop Agreements. and the second is Message Handling System (MHS) as specified by the Workshop Agreements. GOSIP requires the use of Transport Class 4, with the exception that Class 0 is allowed for MHS on public data networks.

Appendices in the current draft GOSIP address advanced requirements (to be included in future versions) through 1990. Areas addressed include Security, OSI Management, Upper Layers, and Lower Layers.

The introduction of GOSIP into the Federal ADP procurement process should accelerate the introduction and development of OSI products not only for the Federal Government but eventually for the private sector as well, just as TCP/IP products developed in the past for the DOD are now readily available for the private sector. GOSIP recognizes the need for OSI management standards and proposes interim solutions until those standards have been developed and implemented.

6.7 X3T5.5

X3T5.5 is the Accredited Standards Committee developing upper layer (above Transport) standards. Their current work involves Upper Layer Architecture (ULA), Transaction Processing (TP), Connectionless Services, Virtual Terminal Protocol (VTP), FTAM, and the standardization of Application Service Elements (ASE).

X3T5.5 is responsible for identifying the upper layer resources and their attributes to be managed. However, it has not yet begun the identification process because of the pressure of other work. When the network management standards become more mature, X3T5.5 is expected to begin this process.

This delay in resource identification is a major problem. Unless this process begins within the next year, delays in the delivery of OSI network management products may occur. Without resource identification, there can be no interoperable network management of upper layer resources.

7 Acknowledgments

The authors would like to thank Dr. Paul Brusil of MITRE Corporation and Dr. Anastase Nakassis and Dr. Dennis Branstad of the NBS for their help and comments in preparing this report. Also, we wish to thank Atul Kapoor of the General Motors Technical Center for his comments on the MAP/TOP section.

8 Bibliography and References

[BRAN86] "Considerations for Security in the OSI Architecture", Branstad, Dennis K., in proceedings of IBM Europe Institute 1986, Oberlech, Austria , Networking in Open Systems, August 18-20 1986

[BRUS87] Brusil, Paul J., "Status: Standardizing Management of OSI Networks", Proceedings of the 6th Annual International Phoenix Conference on Computers and Communications, Phoenix, AZ, February 24-26, 1987, IEEE Computer Society Press

[CMISOV] "Management Information Service Definition Part 1, Overview - Intermediate Working Draft", DP 9595/1, ISO/TC97/SC21/N1372, Egham - September, 1986

[CMISSP] "Draft Proposal of Management Information Service Definition Part 2: Common Management Information Service Definition", DP 9595/2, ISO/TC97/SC21/N1373, Egham - September; 1986

[CMIPOV] "Draft Proposal of Management Information Protocol Specification - Part 1: Overview", DP 9596/1, ISO/TC97/SC21/N1374, Egham - September, 1986

[CMIPSP] "Draft Proposal of Management Information Protocol Specification - Part 2: Common Management Information Protocol", DP 9596/2, ISO/TC97/SC21/N1375, Egham - September, 1986

[CMRP86] "OSI Management Information Services - Configuration Management Rapporteur's Report: Egham 9-11 September 1986", ISO/TC97/SC21/WG4 Egham-10

[CMSD85] "Information Processing - Open System Interconnection - Management Information Service Definition - Part 5: Configuration Management Service Definition", ISO/TC97/SC21 N982, November, 1985

[CMSW86] "Plan for Standardization Work on Configuration Management", ISO/TC97/SC21 N1385. September, 1986

[COSP86] "Corporation for Open Systems. Preliminary Prospectus Dated February 5, 1986."

[DAD286] "Information Processing Systems - Open Systems Interconnection - Proposed Draft Addendum 2 to ISO 7498 on Security Architecture", ISO/TC97/SC21 N931, September 1986

[DIRSER] "ISO/DP 9594, Information Processing Systems - Open Systems Interconnection - The Directory", Parts 1-7, ISO/TC97/SC21 N1376-N1382.

[DIRSEC] "CCITT Draft Recommendation X.ds8 - Directory Systems: Authentication Framework", Version 4, Geneva, October 9, 1986.

[DROS86] "Remote Operations: Model, Notation and Service Definition", CCITT Draft Recommendation X.ros0 (Version 2, Munich, July 1986)

[FMSD86] "Second Working Draft for the Management Information Services Definition -- Part 3: Fault Management", ISO/TC97/SC21 N1383, October, 1986

[FMPS86] "First Working Draft for Management Information Protocol Specification: Part 3 - Fault Management Protocol Specification", ISO/TC97/SC21 N1384 (from Egham), September, 1986

[GOSI86] "Government Open Systems Interconnection Procurement (GOSIP) Specification For Fiscal Years 1987 and 1988". Draft, The U.S. Government OSI User's Committee, December 18, 1986

[IEGL21] "Draft IEEE 802.1 Standard: Glossary", Revision 2/15/86

[IELM23] "WG 802.2 Revised Draft Copy: Layer Management Proposal for 802.2 Section 2.3", July 30, 1986

[IELMDB] "IEEE 802.5 Layer Management, Draft B", July, 1986

[IELMDD] "IEEE P802.3-86/0.05D: Layer Management Draft D", June, 1986

[IELSSM] "Working Draft IEEE 802.1 Network Management Task Group: Layer-Specific Systems Management Guidelines", August, 1986 (To be considered for inclusion in 802.1 Part B: Systems Management as a replacement for the appendix entitled "Layer Management Guidelines")

[IEMANB] "Draft IEEE Standard 802.6 Metropolitan Area Network (MAN) Station Management", Revision B, May, 1986

[IEMCBA] "Draft IEEE 802.1: Part D, MAC Bridges", Revision A, October, 1986

[IEMLM7] "IEEE Draft Standard 802.4 Revision: Section 3: MAC Layer Management, Revision 7", February, 1986

[IEOISM] "Draft IEEE 802.1 Standard: Part A, Overview, Interworking, and Systems Management", Draft D, August, 1986

[IEPLM3] "IEEE Draft Standard 802.4 Revision: Section 9: Physical Layer Management, Revision 3", March 1986

[IESLPA] "Draft IEEE 802.1 Standard: Part B--Systems Management, System Load Protocol", Revision A, September, 1986

[IESMRL] "Draft IEEE 802.1 Standard: Part B, Systems Management", Revision L, August, 1986

[IETGML] "Tutorial Guide to IEEE 802.1 Management Document [Revision L -- Tutorial Version 3.0]", August, 1986

[IS7498] "Information Processing Systems - Open Systems Interconnection - Basic Reference Model", International Standard 7498, International Organization for Standards.

[MGFM86] "OSI - Management Framework - Draft Addendum", DP7498/4, ISO/TC97/SC21/N1371, Egham - September, 1986

[MPNM87] "MAP/TOP 3.0 Network Management Requirements Specification", (To be Released in Early 1987.)

[PFSM86] "Plan for Further Standardization of Management Information", ISO/TC97/SC21 N1387, September, 1986

[ROS186] "ISO/DP 9072/1, Information Processing - Message Oriented Text Interchange System - Remote Operation Service - Part 1: Concepts and Model", ISO/TC97/SC21 N1285

[ROS286] "ISO/DP 9072/2, Information Processing - Message Oriented Text Interchange System - Remote Operation Service - Part 2: Basic ROS", ISO/TC97/SC21 N1286

[SMSD86] "Proposed Draft for Management Information Services Definition, Part 7, Security Management Service Definition", ISO/TC97/SC21 N1386, September, 1986

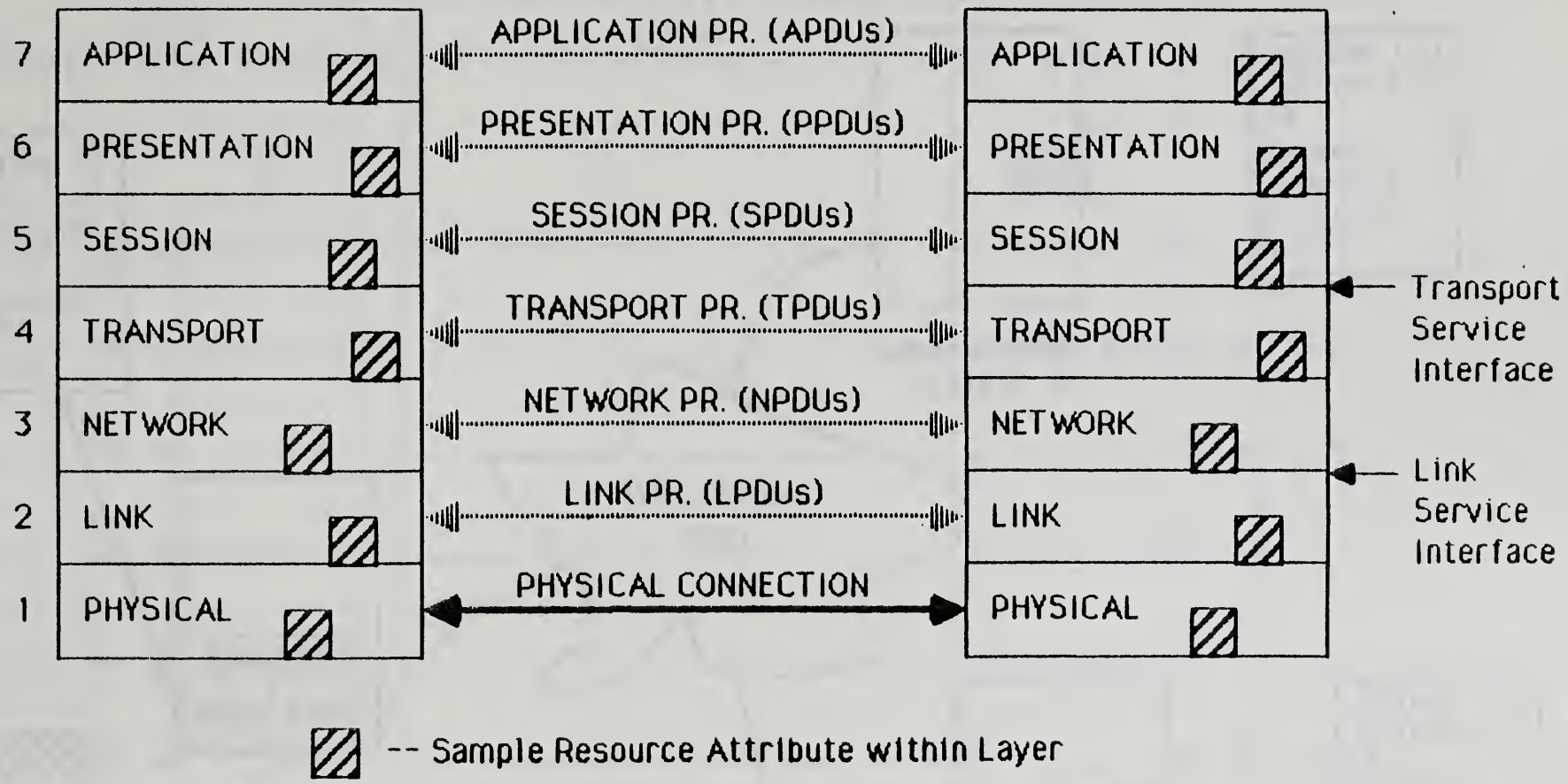
[SC21RP] "Report of the Second SC 21/WG 4 Meeting, Egham, September 4-12, 1986", ISO/TC97/SC21 N1397

[SPNTRE] "An Algorithm for Distributed Computation of a Spanning Tree in an Extended LAN", Radia Perlman, Digital Equipment Corporation, 1984

[S33F86] "Draft Network Layer Routing Architecture", ANSI X3S3.3/86-215

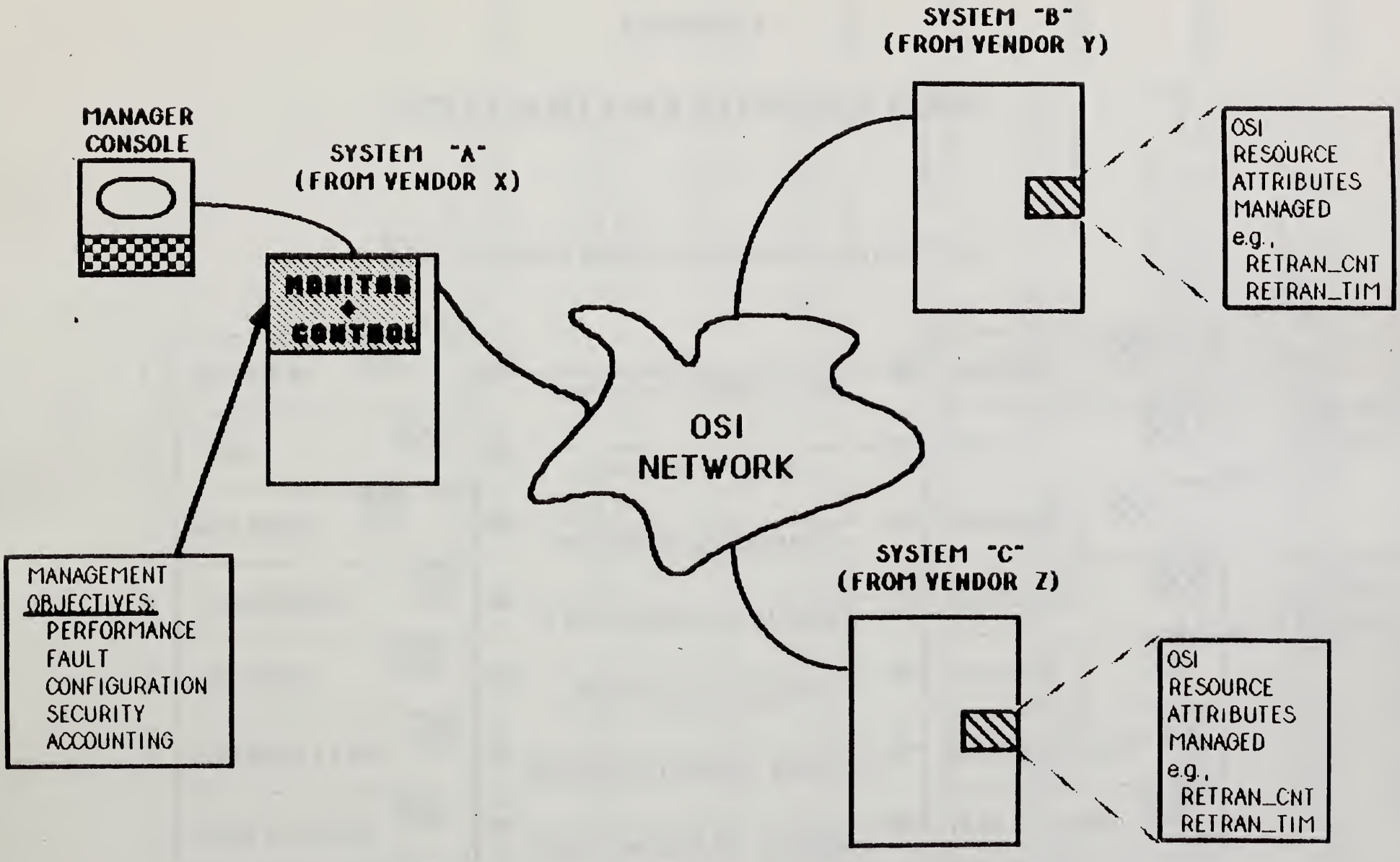
[T54C87] "US Comments on SC21 N1387, "Plan for Further Standardization of Management Information", ANSI X3T5.4/87-27, January 16, 1987

[WOOD86] "Management in OSI", Woodward, B., in proceedings of IBM Europe Institute 1986, Oberlech, Austria , Networking in Open Systems, August 18-20 1986



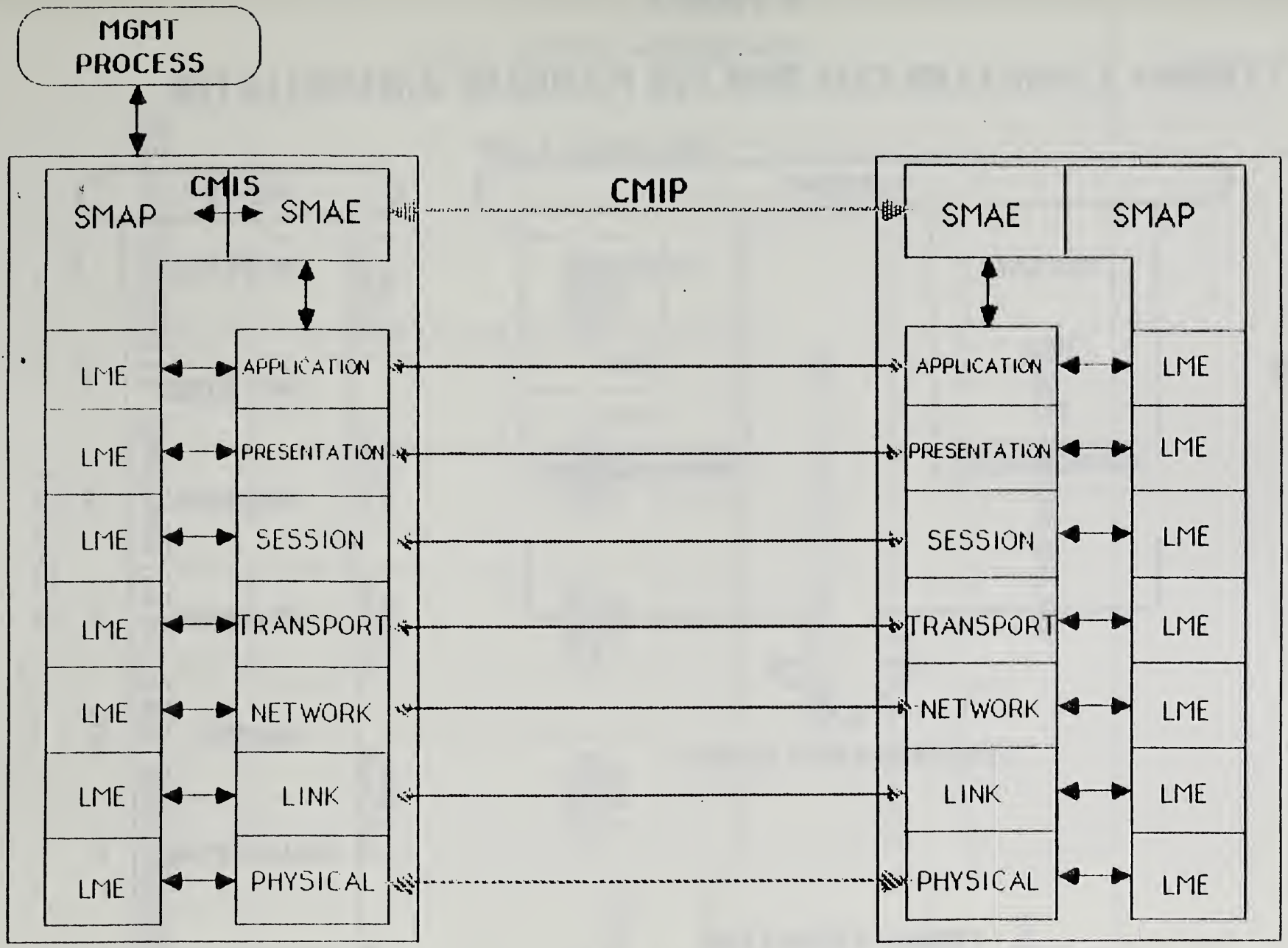
OSI SEVEN LAYER REFERENCE MODEL

FIGURE 1



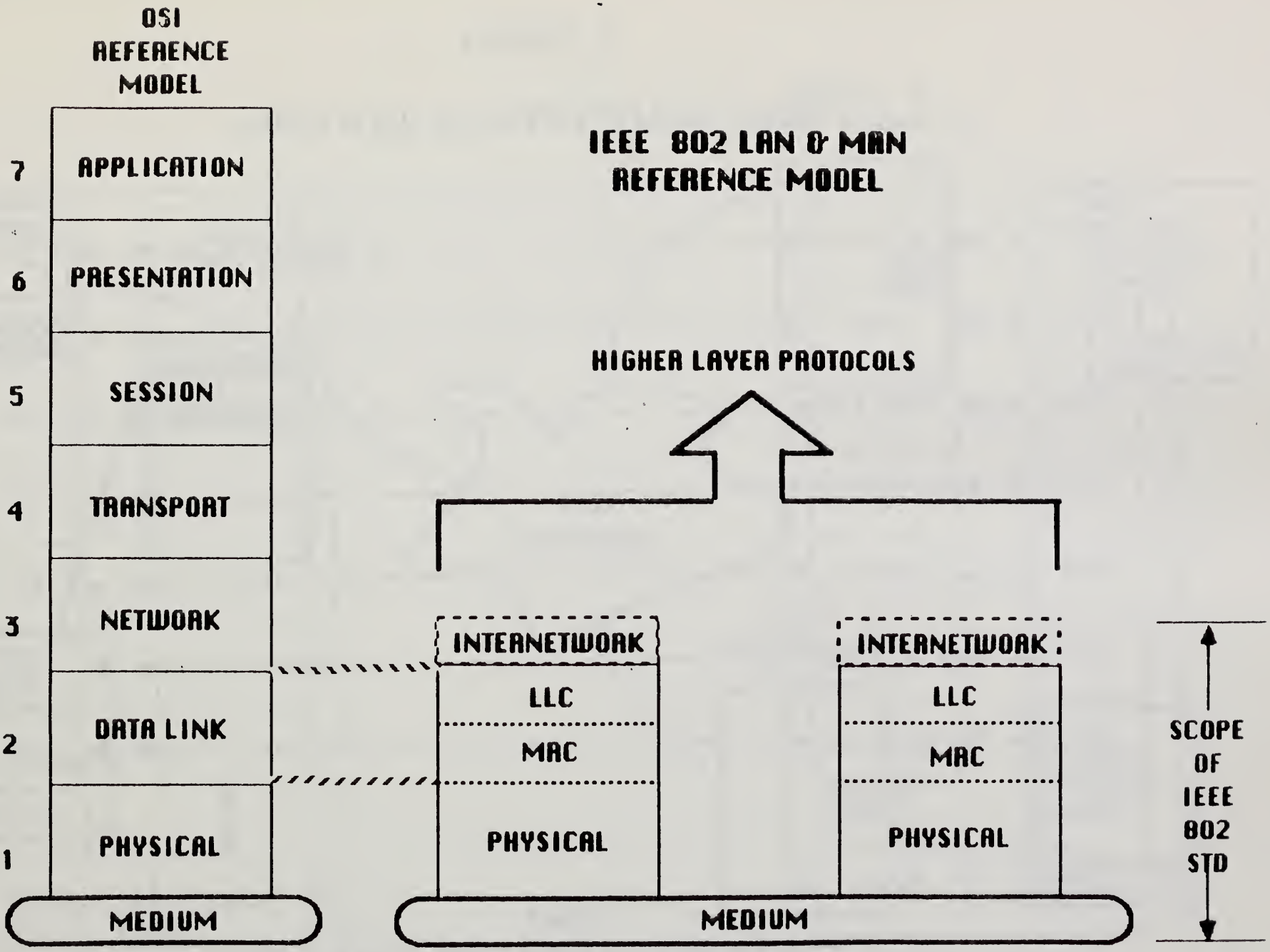
SIMPLIFIED FUNCTIONAL OVERVIEW
OF
OSI NETWORK MANAGEMENT

FIGURE 2



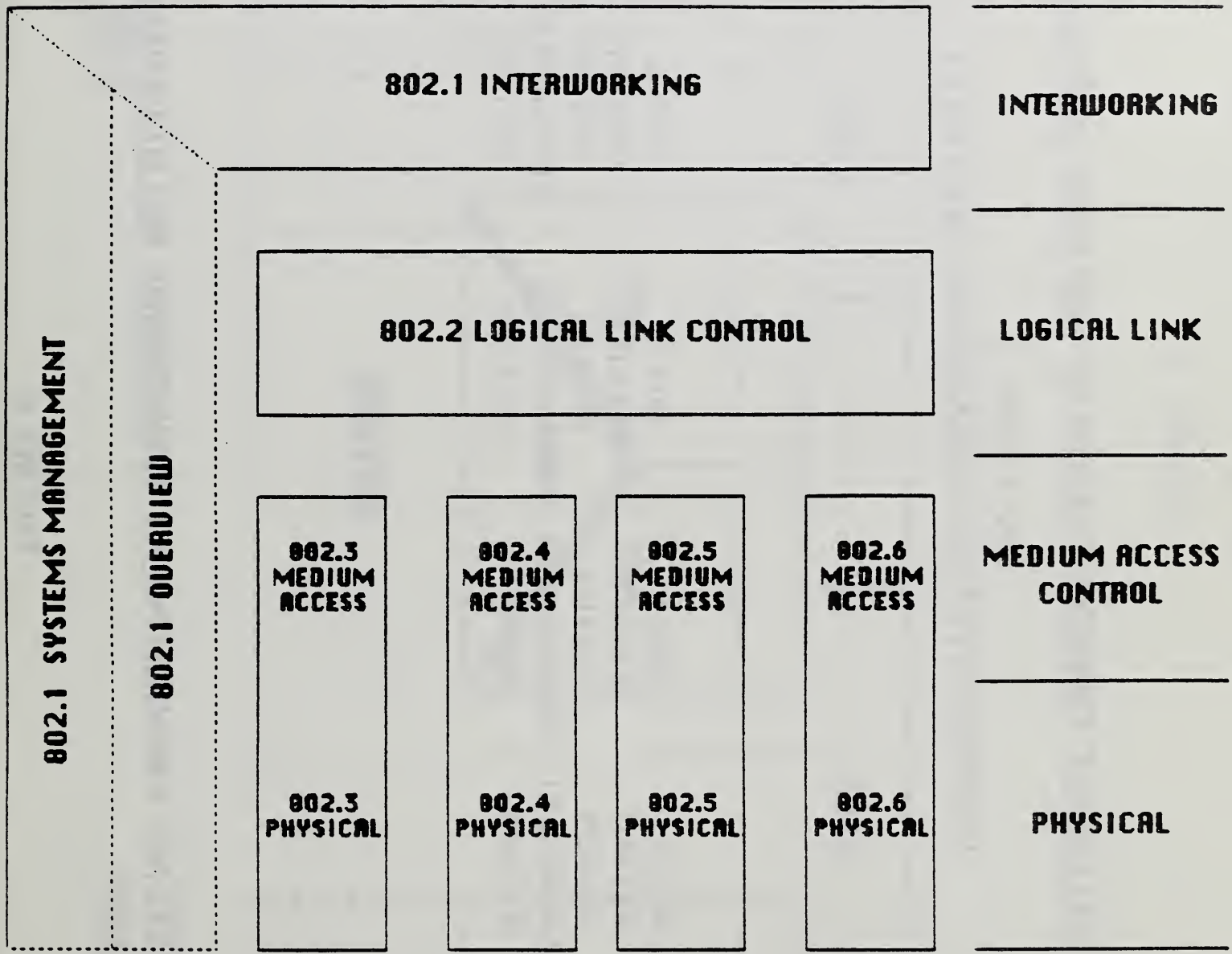
SIMPLIFIED OSI MANAGEMENT MODEL

FIGURE 3



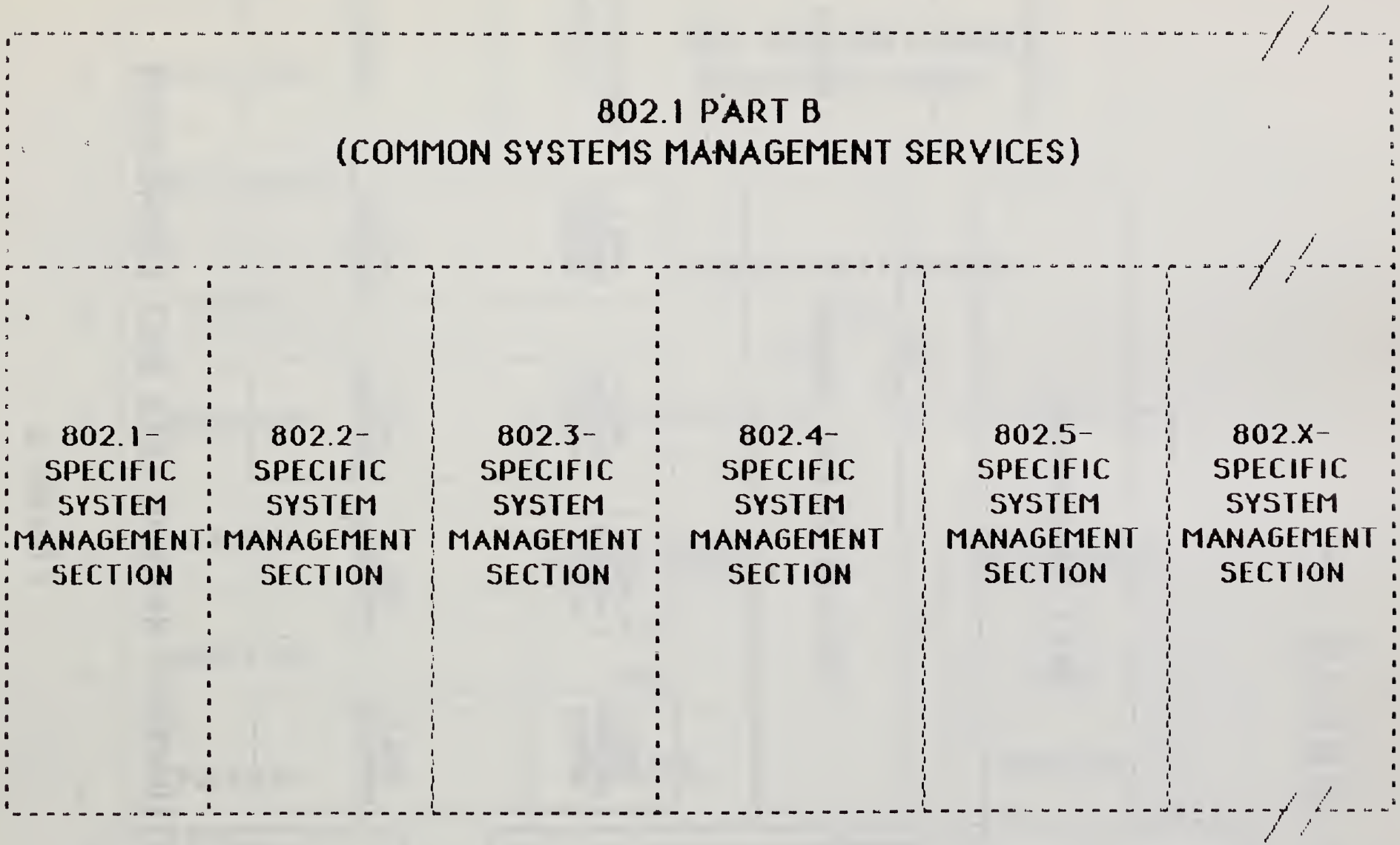
RELATIONSHIP BETWEEN OSI AND IEEE REFERENCE MODELS

FIGURE 4



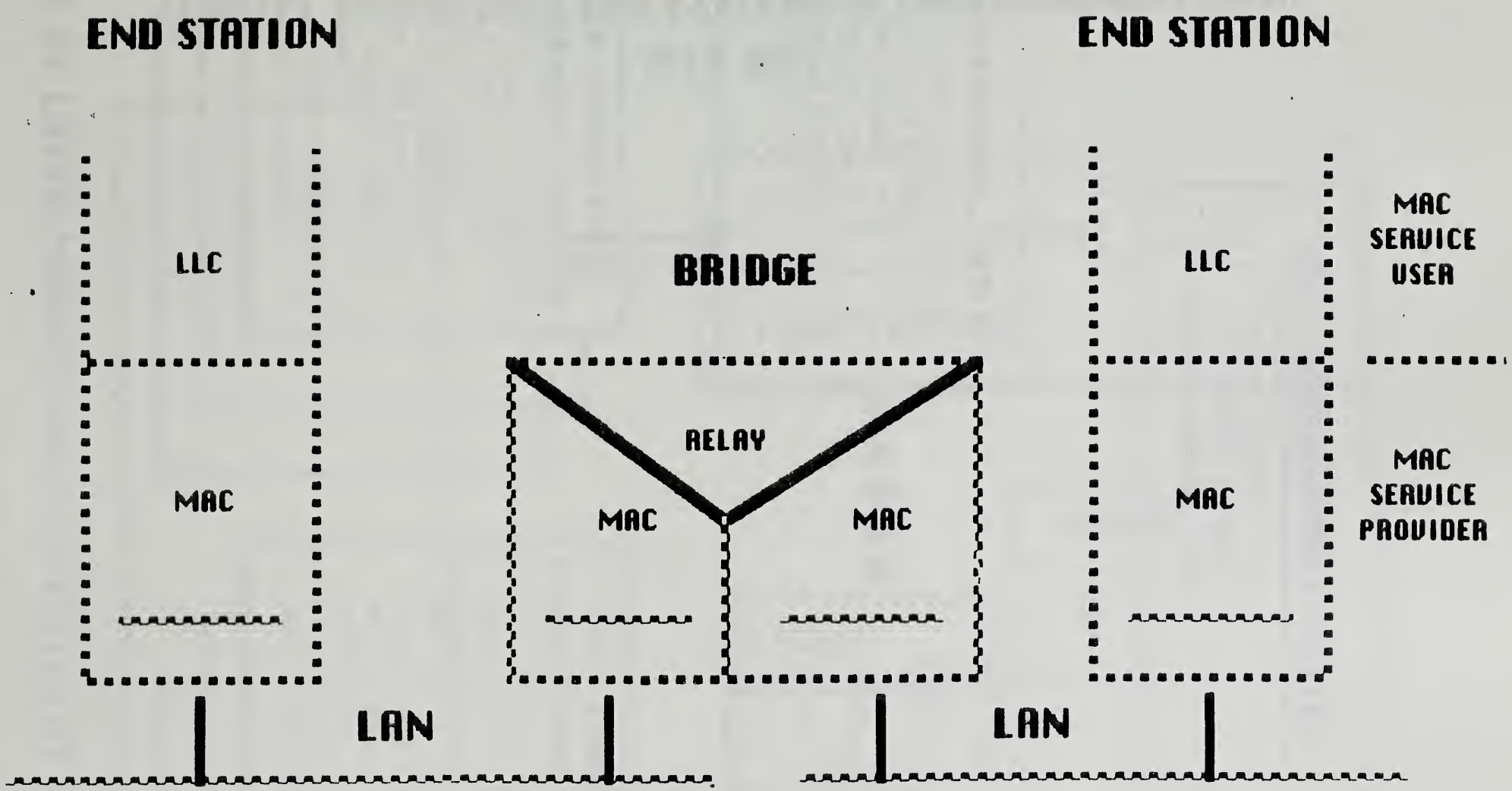
RELATIONSHIP AMONG IEEE 802 STANDARDS

FIGURE 5



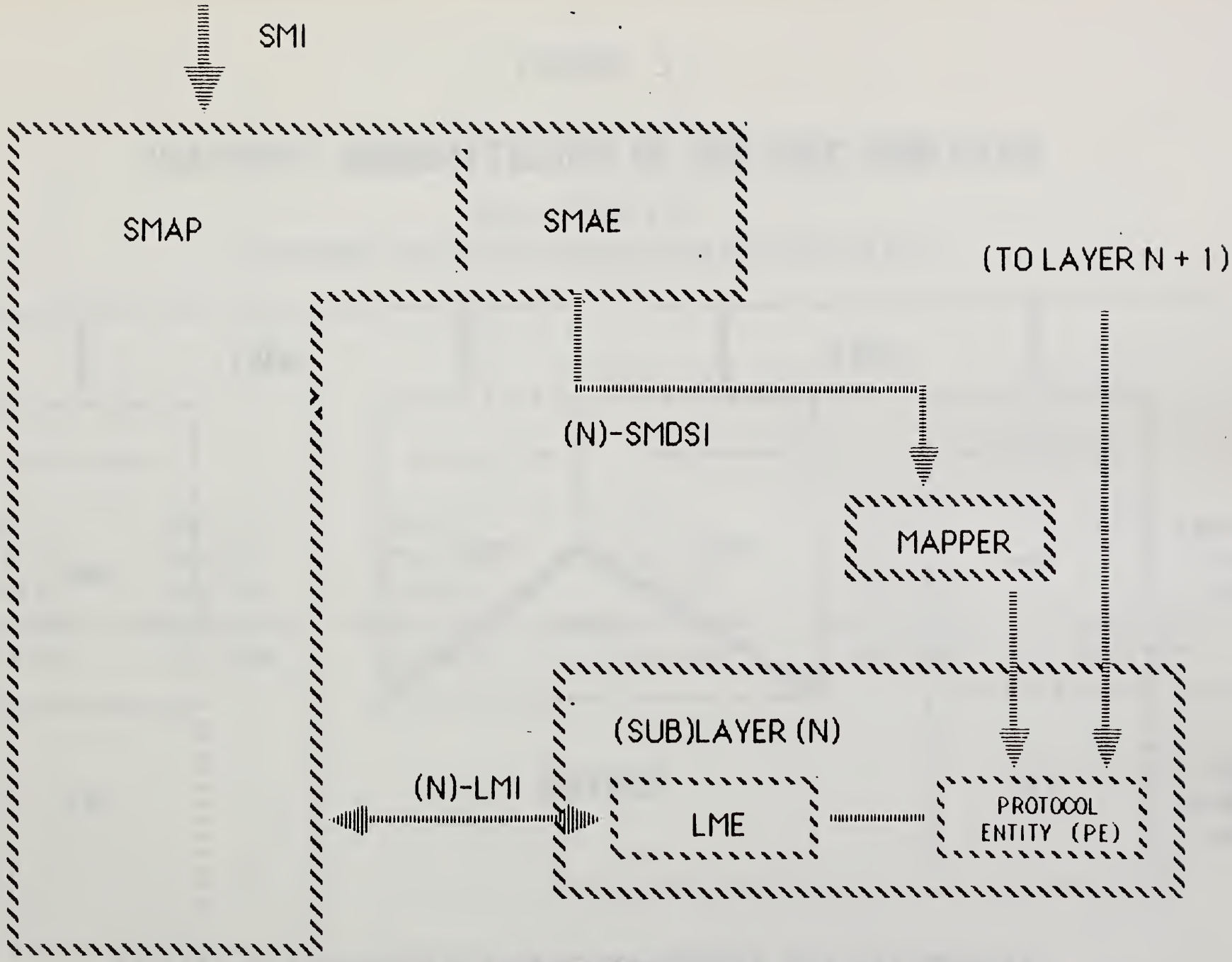
SYSTEMS MANAGEMENT STANDARDS RELATIONSHIP

FIGURE 6



INTERNAL ORGANIZATION OF THE MAC SUBLAYER

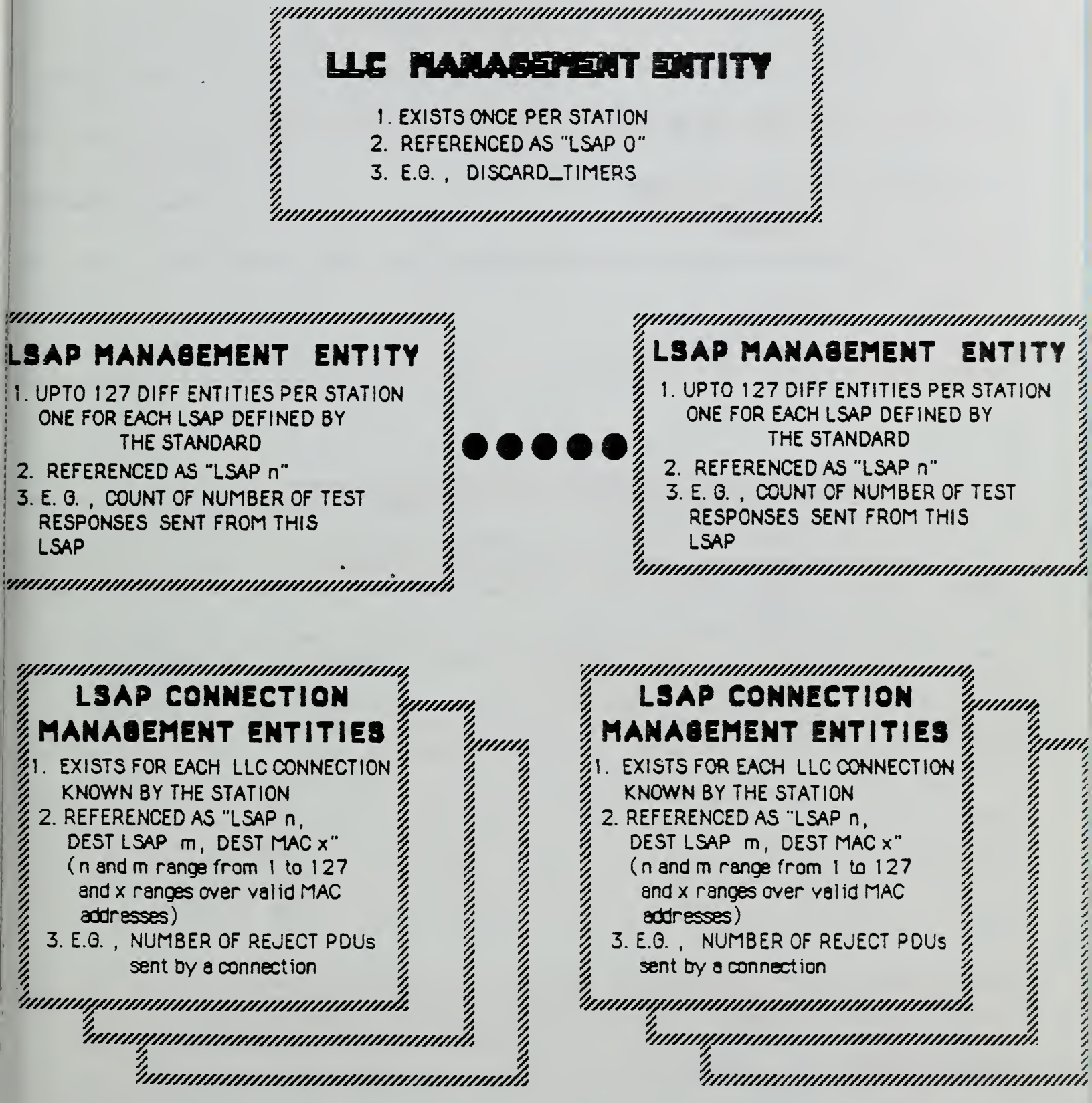
FIGURE 7



IEEE 802

SERVICE INTERFACES FOR SYSTEMS & LAYER MANAGEMENT

FIGURE 8



TYPES OF LAYER MANAGEMENT ENTITIES AT LLC SUBLAYER

FIGURE 9

NBS-114A (REV. 2-8C)

U.S. DEPT. OF COMM. BIBLIOGRAPHIC DATA SHEET (See instructions)	1. PUBLICATION OR REPORT NO. NBSIR 87-3593	2. Performing Organ. Report No.	3. Publication Date AUGUST 1987

4. TITLE AND SUBTITLE

A Survey of OSI Network Management Standards Activities

5. AUTHOR(S)

C. Michael Chernick, Kevin Mills, Robert Aronoff, John Strauch

6. PERFORMING ORGANIZATION (If joint or other than NBS, see instructions)

NATIONAL BUREAU OF STANDARDS
U.S. DEPARTMENT OF COMMERCE
GAITHERSBURG, MD 20899

7. Contract/Grant No.
#OCH-4-001

8. Type of Report & Period Covered
Final

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (Street, City, State, ZIP)

Thomas Powis
ULANA Program Manager
AFLANSPO, HQ ESD/OCC-2
Hanscom AFB, Hanscom, MA 01731

10. SUPPLEMENTARY NOTES

☐ Document describes a computer program; SF-185, FIPS Software Summary, is attached.

11. ABSTRACT (A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here)

This paper surveys the status of OSI network management activities. The executive summary projects future availability of standards and commercial products for the management of OSI systems. Several major problems remaining to be solved by the standards community, are discussed.

The OSI seven layer model is reviewed with particular emphasis on explaining the concept of interoperable, vendor-independent network management. The need for management of resources at each layer is presented.

The roles of organizations important to the development of network management standards are explained. These organizations include ANSI (X3T5.4, X3T5.1, X3S3.3), IEEE 802, and MAP/TOP. The models of network management used by each of these organizations are briefly discussed and the status of their major documents is reviewed.

The paper reviews the characteristics and capabilities of the specific management areas described in the ISO management framework model. These management areas include: Configuration and Name Management, Security Management, Performance Management, Fault Management, and Accounting Management. The Common Management Information Service (CMIS) and Common Management Information Protocol (CMIP) and their capabilities are reviewed.

A bibliography of relevant standards papers relating to OSI Network Management, as of March, 1987, is provided.

12. KEY WORDS (Six to twelve entries; alphabetical order; capitalize only proper names; and separate key words by semicolons)

Computer Network Management; Computer Network Protocols; Computer Network Protocol Status; Computer Network Protocol Survey; Computer Network Standards; Open Systems Interconnection;

13. AVAILABILITY

☒ Unlimited
☐ For Official Distribution. Do Not Release to NTIS
☐ Order From Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.
☒ Order From National Technical Information Service (NTIS), Springfield, VA. 22161

14. NO. OF PRINTED PAGES
58

15. Price
$13.95

USCOMM-DC 6043-P80