prices. There is debate, however, concerning the effectiveness of competition in assuring high reliability for these services. Competition may influence a developer to market a product before it has been thoroughly tested. Some analysts speculate that regulation may be necessary to assure acceptable reliability and that some regulation to require that certain basic technologies be available for users at reasonable prices may be beneficial. Many, general examples could be cited, however, to argue that regulation often stifles innovation, reliability, and economy.

On the other hand, the development of standards is, in fact, a process that is supported extensively by organizations that provide network facilities and services, as well as organizations that develop and market both hardware and software for network management. The necessity of competition in the market place may influence and even restrict their willingness to completely and cooperatively support the agreements that would provide for "ideal" standards that would be completely consistent and sharply focused.

3. NETWORK MANAGEMENT STANDARDS

What are standards? Who needs them? Who makes them? How? What about network management standards? What are the current NM activities? What are the future issues and trends in standards for network management? The purpose of this section is to address these questions.

Standards for telecommunications have been evolving for many years. However, in the 1980's, the demand for standards increased as divestiture became reality and technology advanced, network users increased, and networks took on global statures. The expanding technical innovations resulting from the convergence of telecommunications and computer technologies also played a key role.

In order to meet the need for standards, there are numerous organizations dedicated to standards development. The complex nature of these global, regional, and national organizations involved with information processing and telecommunications standards is depicted in Figure 14, developed by A. M. Rutkowski of the International Telecommunications Union (ITU) (Knight, 1991). Table 5 provides definitions of the many acronyms used in Figure 14. The arrows between organizations indicate the relative information flows and interworking.

Until recently, most participants in the standards-setting organizations were representatives of the telecommunications providers. Users were seldom represented. Participants came together

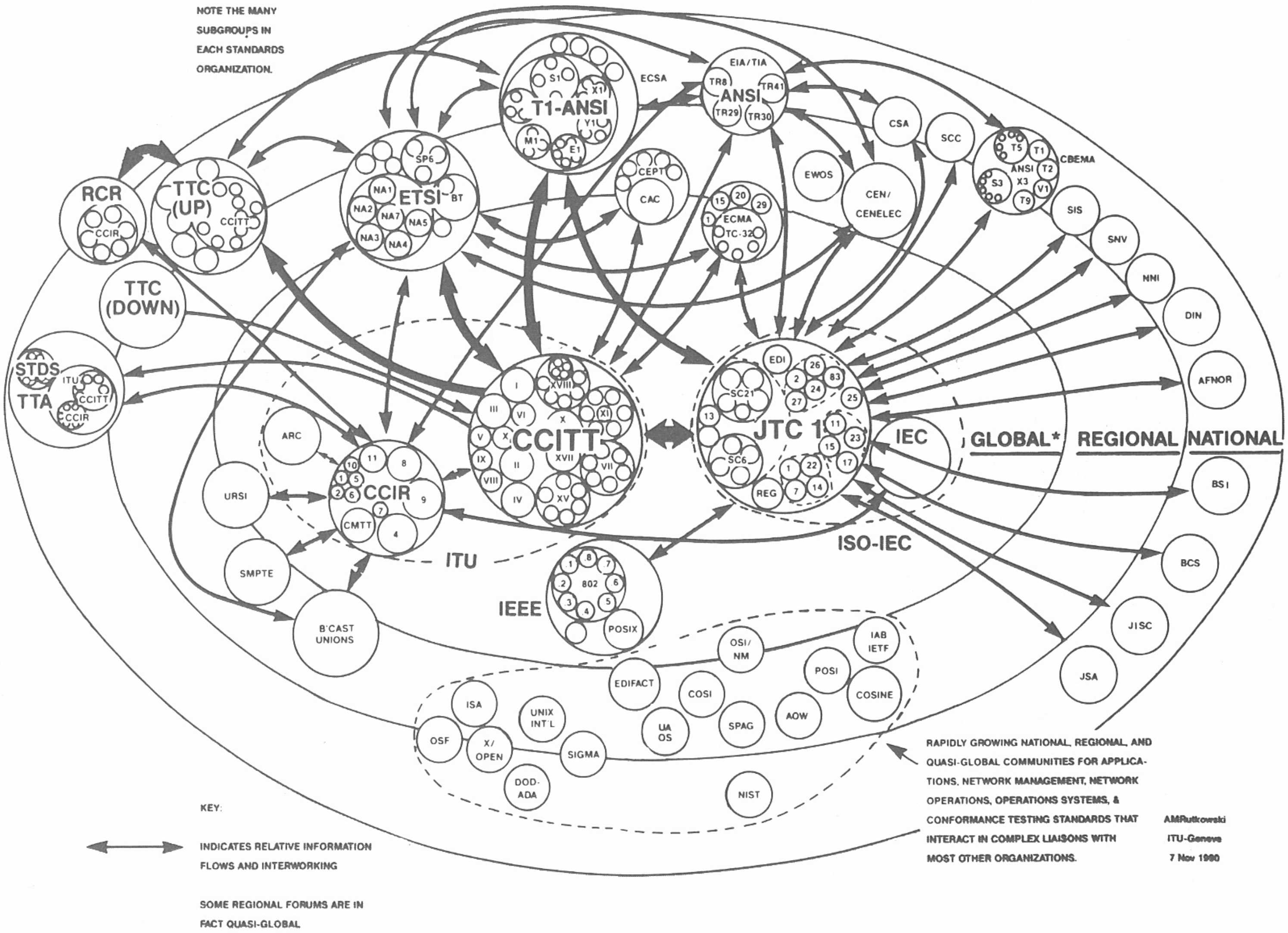


Figure 14. Global, regional, and national standards organizations (Knight, 1991).

Table 5. Acronyms Used in Figure 14

AFNOR	Association francaise de normalisation
ANSI	American National Standards Institute
AOW	Asian-Oceania Workshop
ARC	Administrative Radio Conference
BCS	British Computer Society
BSI	British Standards Institute
CCIR	International Radio Consultative Committee
CCITT	International Telegraph and Telephone Consultative Committee
CEN/CENELEC	Comite Europeene de Normalisation Electronique
CEPT	European Conference of Postal and Telecommunication Administrations
COS	Corporation for Open Systems International
COSINE	Corporation for Open Systems Interconnection Networking in Europe
DIN	Deutsches Institut fur Normung
DoD-ADA	U.S. Department of Defense - ADA Joint Program Office
ECMA	European Computer Manufacturers Association
ECSA	Exchange Carriers Standards Association
EDIFACT	Western European Electronic Data Interchange for Administration, Commerce, and Transportation
EMUG	MAP/TOP Users Group
ETSI	European Telecommunications Standards Institute
IAB/IETF	Internet Activities Board/Internet Engineering Task Force
ISA	Integrated Systems Architectures
ISO	International Organization for Standardization
ITRC	Information Technology Requirements Council
JISC	Japan Industrial Standards Association
JSA	Japan Standards Association
JTC1	Joint Technical Committee 1 - Information Technology
NIST	National Institute for Standards and Technology
NNI	Nederlands Normalisatie-instituut
OSF	Open Software Foundation
POSI	Pacific OSI Group
RCR	Radio Council for Research
SAA	Standards Association of Australia
SCC	Standards Council of Canada
SIGMA	[Unix Open Applications Group - Japan]
SIS	Standardiseringskommissionen I Sverige
SMPTE	Society of Motion Picture and Television Engineers
SNV	Swiss Association for Standardization
SPAG	European Standards Promotion and Applications Group
T1	Standards Committee T1 - Telecommunications
TTA	Telecommunication Technology Association of Korea
TTC	Telecommunications Technology Council
UAOS	Users Association for Open System

to discuss and sometimes agree on standards or recommendations. Controversy somtimes arose over respective areas of responsibility and membership roles. Figure 15 is a greatly simplified version of some important standards making processes. Three principal areas are indicated with some common overlap. Telecommunications organizations are concerned primarily with standards for voice and integrated service networks. The radio organizations deal with satellite systems, cellular radio networks, land mobile radio, and personal radio communication networks. Computers and information processing standards organizations cover local and wide area networks, high level protocols, and open systems.

In the past, the organizations developing various standards have tended to restrict their activities to their own domains. More recently the technical innovations resulting from the convergence of telecommunications, computers, and information processing has led to more areas of common interest and, in some cases, conflict. This conflict has arisen because of the inherent competitive nature of these industries. For example, the computer industry strives to put more and more intelligence in the terminals whereas the telecommunication industry would prefer to imbed intelligence in network nodes (i.e., switches, transfer points, and data storage elements).

For example, the ISO/IEC Information Processing Standards and ANSI X3 Committees are mostly concerned with information processing functions and their protocols. Emphasis is on bringing more of these functions to the user terminals and host computers. The tendency is to view communications as a pipe between computers and terminals. The CCITT study groups place more emphasis on putting the processing functions inside the network at the switching nodes and, thereby, reducing the burden on the user terminals.

The advent of personal communication systems or universal personal telecommunications (UPT)[21] brings the radio industry into this standards picture. Resolution of the technical, political, standards, and regulatory issues regarding PCS could have a long-term impact on the basic structure of telecommunications in the 21st century. Prospects for PCS, as an alternative to the PSTN, are discussed by Bryan (1991).

Various kinds of subcommittees, study groups, and joint working parties are involved in the standards making processes. Participants include service providers, manufacturers, vendors,

[21] PCSs evolved from cellular mobile technology to support voice and low-bandwidth data in hand-held, portable communicators. UPT requires an intelligent network that supports person-to-person telecommunications including voice, data, fax, and video.

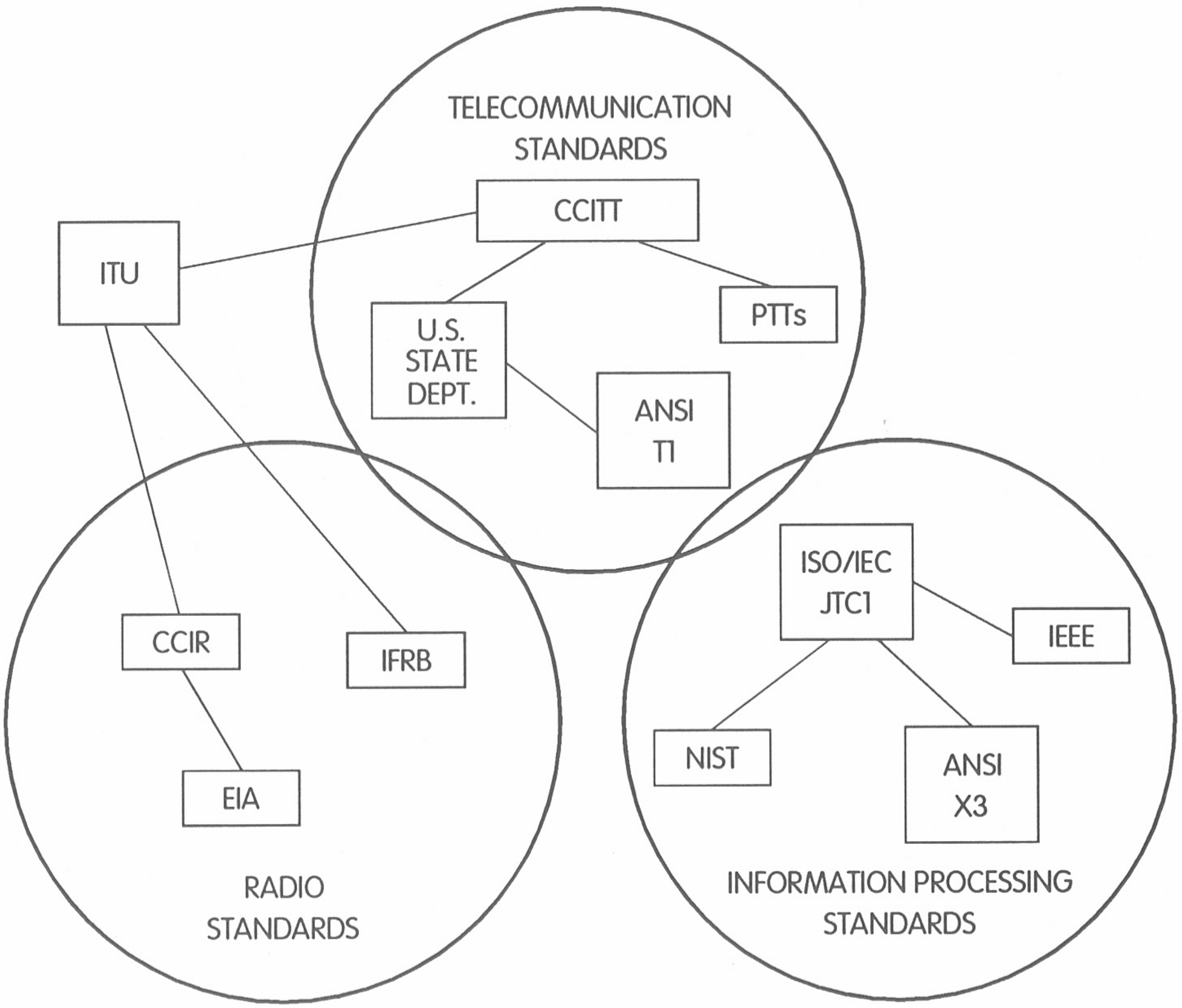


Figure 15. Major groups involved with standards for telecommunications and information processing.

users, and government administrations. Some groups include only one category of participants whereas others may include several categories. Three types of groups are involved in the standards making process. First are the telecommunications industries themselves who develop so-called industrial standards. Then, there are organizations whose primary purpose is developing standards so competing vendors' equipments are compatible or can be interconnected to the same network. Finally, there are groups whose purpose is to develop coherent standards prior to actual system implementations. Ultimately, the approved standard is intended to exert control over the computer and communications markets.

The standards-making process is discussed in Section 3.1. Organizations involved in this process are described in Appendix A. Current activities by organizations involved with the development of network management standards are covered in Section 3.2.

3.1 The Standards Making Process

This section is concerned with the standards-making process in general and with network management standards in particular. The concern here is with the full range of networks to be managed including LANs, wide area networks (WANs), national and international networks, public and private voice networks, and packet data networks. Network management standards are being developed by various national and international standards organizations including the ISO and the CCITT. The ISO is concerned with international information processing standards and the CCITT with ISDN and international telecommunication standards. The ISO is concentrating on how to manage Open System Interconnection (OSI) networks. The CCITT emphasis is on the management of telecommunications network elements such as switching nodes, multiplexors, and transmission facilities.

In the following subsections, we describe the needs for standards (3.1.1), the standards-making process (3.1.2), the players in the process (3.1.3), and finally NM standards (3.1.4). Appendix A describes the organizations involved with NM standards and their relationship with each other. The complex, standards-making process can be fully understood only by understanding the relationships between the needs for standards and the organizations involved with developing the standards.

3.1.1 The Need for Standards

Before discussing the process for developing standards it is useful to define what is meant by ‘standard’ and who needs them. Cargill (1989) defines standards as follows: "A standard is the deliberate acceptance by a group of people, having common interests or backgrounds, of a quantifiable metric that influences their behavior and activities by permitting a common interchange."

For telecommunication standards there appear to be two viewpoints of standards—one technical and the other functional. The technical view is that two pieces of equipment are standardized if they can interoperate or each be used with the same interconnection. The alternative functional view is that the documented standard specifies approved means of accomplishing a set of tasks or functions, i.e., a more general specification of functional capability. In this case different implementations may produce equipment that meets the standard but that will not interoperate or be interchangeable because the individual manufacturers have followed different implementation options.

Some other benefits for telecommunication and information-processing standards are market driven. These include interchangability, convenience, risk reduction, interconnectibility, safety, ease of use, and technical integration.

The following noteworthy comments, derived from various sources, indicate the need for standards:

- Standards-setting has become a factor with important implications for competition.

- Standards developed *a priori* increase the chances for increased worldwide compatibility before large competitive investments.

- Standards are supported by network users because standards give them control over the technology and allow the development of open systems.

- Standards will profoundly effect the balance of power in key relationships within the computer and communications industries by giving users more choices and making it easier to substitute equipment.

- Standards usually are consensus statements by committees whose members believe their work will be understood, accepted, and implemented by the market.

- International standards provide opportunities for promoting National technological leadership.

- Standards provide the means for integrating services over telephone networks and internetting computers over data networks.

3.1.2 The Standards Making Process

The development of standards is a multistep process (Cargill, 1989). One simplified example of the general process is shown in Figure 16. An estimated time scale for the major steps in these processes is given on the left side of the figure and examples of some organizations involved with each step are listed on the right. The process begins with the establishment of a need or requirement. This may come from a variety of sources including service providers, equipment suppliers, and the users. Each group may approach this need from a different perspective. The providers, for example, tend to view their networks as all encompassing, capable of meeting a variety of users needs, and having a long productive lifetime. The users on the other hand are interested in an immediate implementation to meet a specific application. (See Section 3.1.3.) Needs may also evolve from special groups formed for that purpose. For example, the International Federation for Information Processing (IFIP) tends to be a pre-standards organization that investigates only the need for standards, not their development.

The next step in this sequence is to develop a basic framework and models for standards development. This framework scopes out the standardization activities needed to develop a particular standard or set of standards, e.g., for network management. This framework provides an overview of what is, and what is not, being standardized. Detailed models then refine the basic framework. Finally, a functional architectural model leads to standards development by national and international organizations. These organizations typically concentrate on standards for specific environments such as local area networks, or long-haul networks. See Appendix A. Some are concerned with terminal access to transmission systems, some for computer communications, others for ISDN and telephony. The ultimate goal of these standards is to enable the development of interoperable, multivendor products for information processing systems and telecommunication networks.

Once the standards are developed, accepted, and promulgated by industry providers, other user-oriented organizations must develop specifications which identify the options (or profiles)

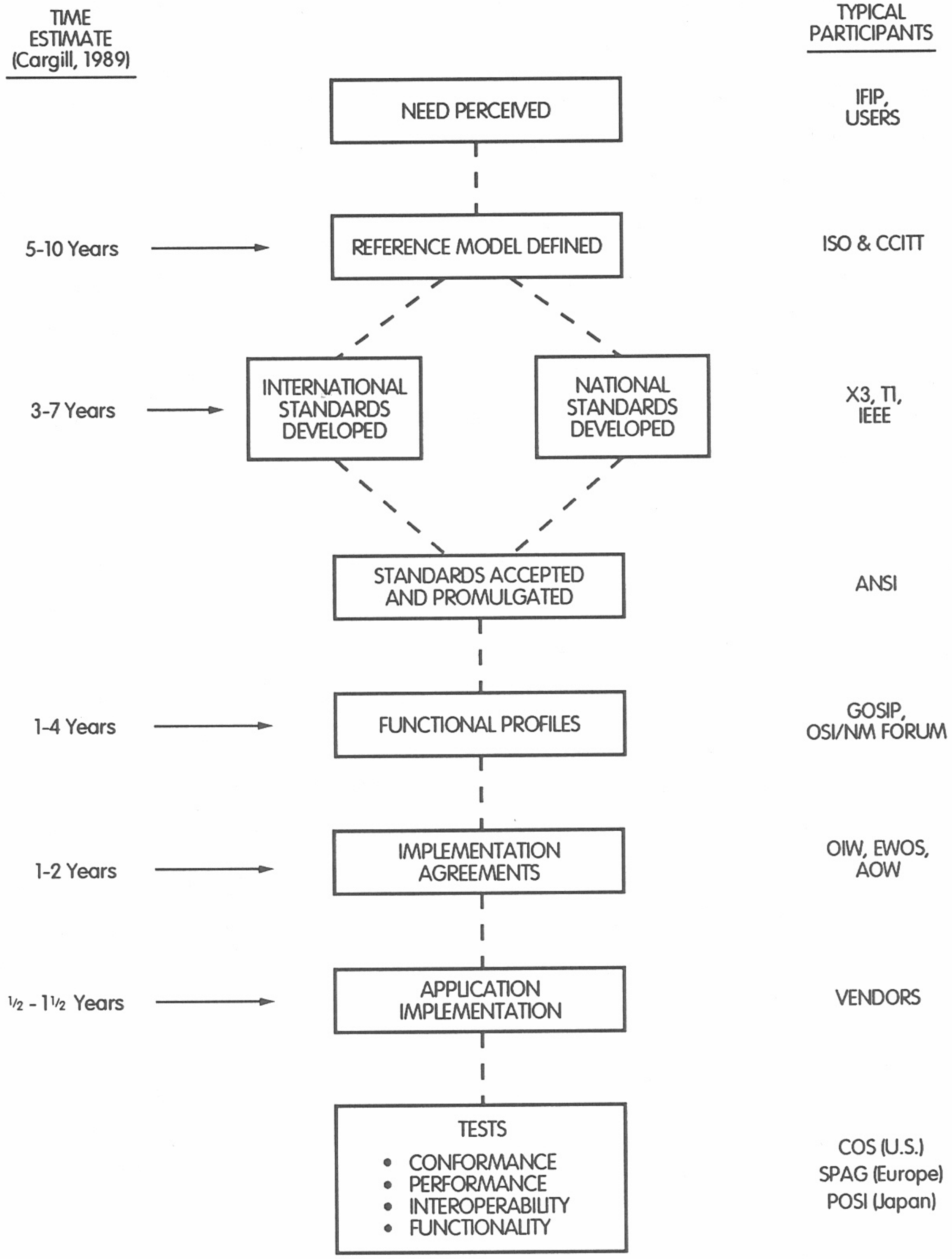


Figure 16. A model for the standards-making process.

and sets of protocols (often called protocol profiles or suites) that a given implementation should support. Separate functional profiles may be needed for different applications (e.g., electronic mail, file transfer, or network management) and for different networks (e.g., physical or virtual, connection-oriented or connectionless). These profiles are actually cross-sections of functional applications pertaining to a particular environment. The functional profile specifies the sets of functions that are to be implemented and how they should appear to external systems. There are many possible ways to implement a profile in hardware and software, but, externally, the functions should all appear identical. As an example, the Government's Open System Interconnection Protocol (GOSIP) defines Federal procurement profiles for open system (OSI) computer network products. Such profiles may change as technology improves and as standards evolve. New profiles are added as new applications arise.

Profiles may be derived from many sources and various architectures. Some vendors have profiles based on their proprietary architectures such as the SNA used in IBM networks. The profile is used to provide interoperability not the use of an 'open' architecture. But interoperability still requires agreements on how the profiles should be implemented. These so-called implementation agreements (IAs) or system profiles are derived by consensus among users, vendors, and system integrators at various forums and workshops both national and international. For example, the OSI Implementors Workshop (OIW), that is sponsored by NIST and the IEEE Computer Society, is developing IAs for emerging network management standards. Implementors workshops including those in Europe and Asia may submit profiles to the ISO which can issue International Standardized Profiles (ISPs).

Products implemented according to the IAs must then be tested to certify that they meet specifications. The several kinds of testing include

Conformance Testing to verify that an implementation acts in accordance with a particular specification (e.g., GOSIP).

Performance Testing to measure whether an implementation satisfies the performance criteria of the user.

Functional Testing to determine the extent to which an implementation meets user functional requirements.

Interoperability Testing to ensure that implementations by various providers will work together properly in the intended environment.

Most vendors had not yet had their equipment certified for compliance with established standards in 1991 because testing agencies were still in the process of establishing criteria for compliance testing and certification. A number of specific national and international organizations are working actively to evolve this type of testing criteria. One is the Corporation for Open Systems (COS), a U.S.-based agency developing tests for the OSI Reference Model's Layers 1 through 4, which deal with physical, data link, network, and transport services and protocols. Another is the Standards Promotion and Applications Group (SPAG), a European group establishing tests for Layers 5 through 7, dealing with session, presentation, and application services and protocols. Yet another is NIST which is overseeing the setting of standards for GOSIP. A general understanding of the testing processes for the ISDN is given by Su and Collica, (1991).

An approximate time scale, given by Cargill (1989), for developing a standard is shown on the left side of the diagram in Figure 16. The entire process is estimated to take anywhere from 11 to 22 years. Of course, the process is never complete since changes occur and new standards evolve as technology and needs change. Examples of the organizations involved in the standards-making process are shown on the right side of Figure 16. These organizations are discussed in more detail in Section 3.2 with emphasis on those groups concerned with network management.

3.1.3 Players in the Process

Key to the standards-making process are the participants and the immense diversity they bring to the standards organizations. The committees, subcommittees, working groups, study groups, and task groups are composed of experts from industry, users, manufacturers, government, and academia, as well as individual experts. These are the players who introduce concepts, establish needs, debate and resolve issues, and ultimately reach a consensus. In order to participate in the process, individuals and their organizations usually must indicate an interest, pay a nominal fee for membership, and attend meetings.

The following quotation from Cargill (1989) indicates how participants impact the standards-making process and the difficulty of obtaining workable and acceptable standards within a reasonable time frame.

> "Imagine a typical international standards meeting where work is being performed on a conceptual/process standard for the information technology industry. Assume a small meeting of approximately thirty representatives—say, twelve from providers, eight from government, five from impacted users or quasi-governmental bodies, several consultants, and a couple of academics. They consider the national, regional, and international aspects of the meeting, the needs of the providers to ensure that their processes are not compromised, the governmental issues such as security and national prestige and protection of industry, and the academic section's insistence on a good and technologically sound solution. Finally, factor in the personal characteristics of the delegates, most of whom are highly competent engineers who have been working on this type of technological problem for years and for whom this arena is a chance to air their theories to their peers. Each individual represents herself/himself, an affiliated group (user, providers, government), a specific discipline (hardware, software, electrical engineering, computer science, marketing, legal), national and regional positions, and the specific company or user group that funded her/him at the meeting. It is easy to see why tidy definitions collapse in the face of so many different interests."

The major players in this process are network users, suppliers, and service providers with subgroups as shown in Figure 17. We will include government and academia in the user category and include all of the suppliers into the service provider category since their viewpoints are similar. Using this dual user/provider categorization, we then examine the important differences between viewpoints in the standards making process. Figure 18 depicts these differences. Service providers tend to take a global, all-encompassing view of the network. From their perspective, the network design should satisfy the diverse needs of various users for a long time. This perspective evolves from competition and the need to reduce implementation, operation, and maintenance costs. The users, on the other hand, take a much more restricted viewpoint. Users are interested in either one or very few specific applications and desire implementation in a short time. Other user/provider distinctions are shown in Figure 18. These distinctions result in different approaches by these two groups in the standards-making process.

Until 1984, the AT&T was the primary source for "de facto" standards in the United States. Then, as a result of divestiture, long-distance and local-area services were redefined as separate businesses and enhanced services beyond POTS were regulated differently. This situation has fragmented the United States market into a multiple-network structure, increased the need for new standards organizations, and complicated the user/provider relationship, but made manufacturers and suppliers from all over the world more competitive. The administrative

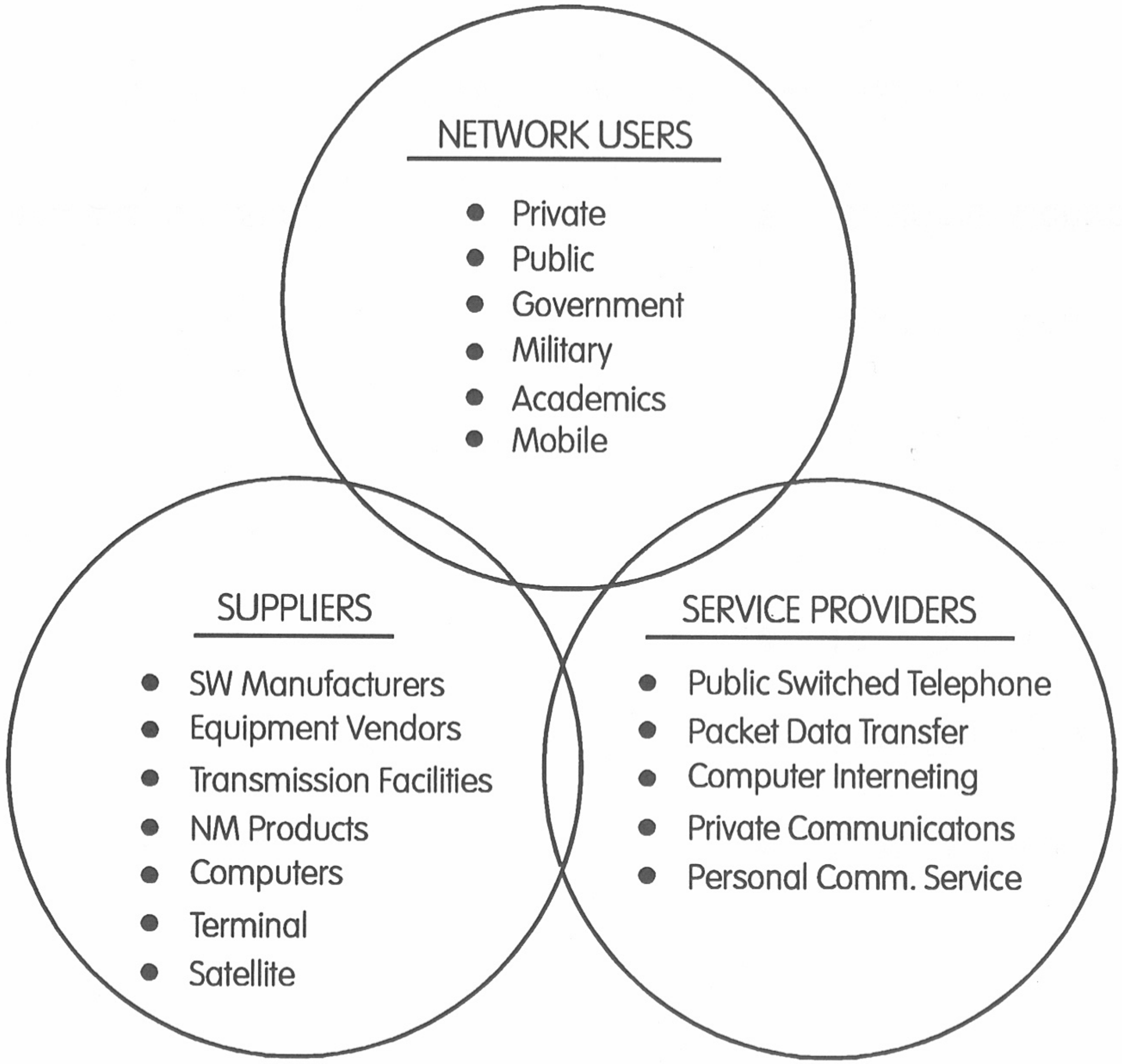
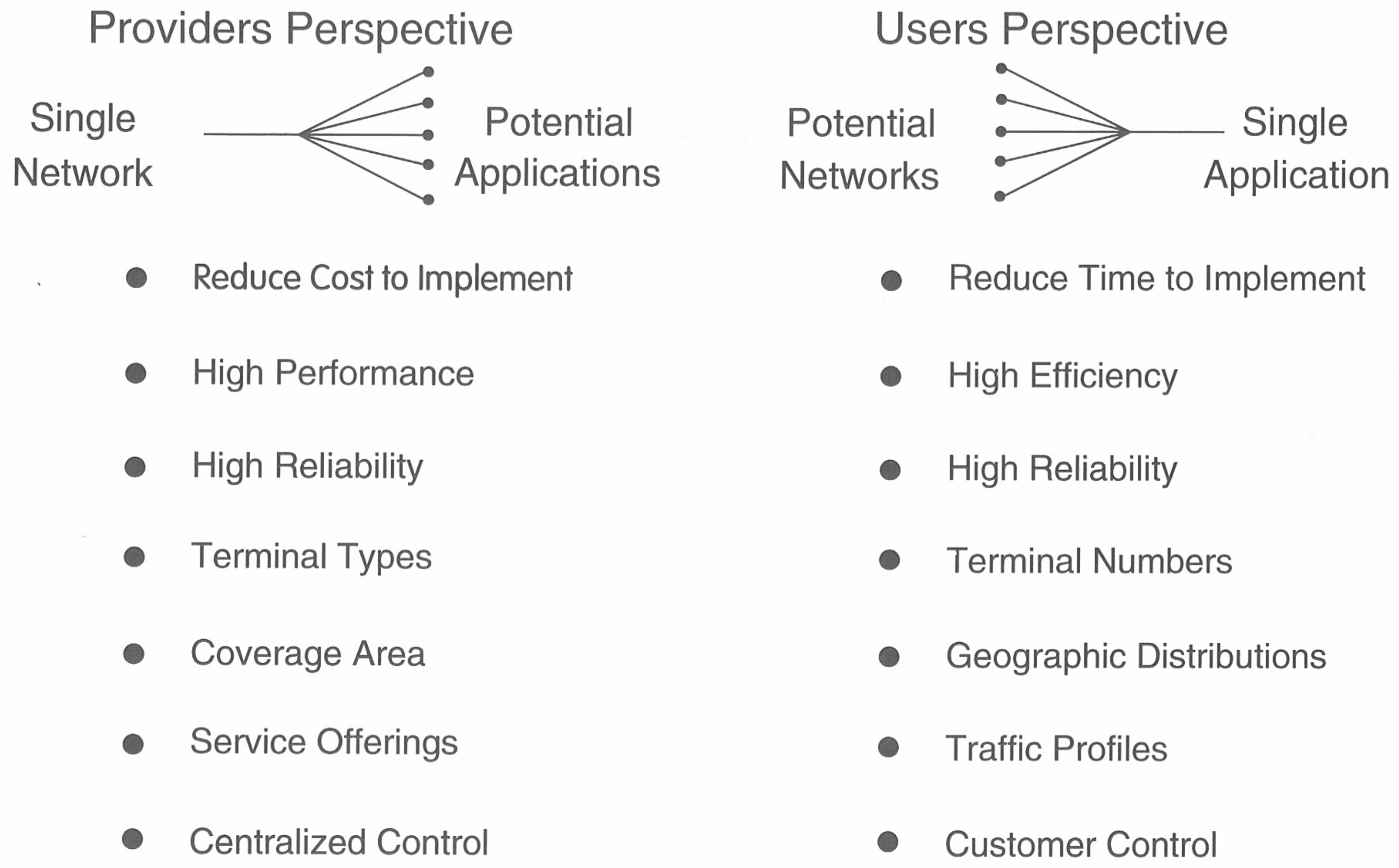


Figure 17. Major participants in the standards-making process.



Providers Perspective	Users Perspective
Single Network — Potential Applications	Potential Networks — Single Application
● Reduce Cost to Implement	● Reduce Time to Implement
● High Performance	● High Efficiency
● High Reliability	● High Reliability
● Terminal Types	● Terminal Numbers
● Coverage Area	● Geographic Distributions
● Service Offerings	● Traffic Profiles
● Centralized Control	● Customer Control

Figure 18. Critical distinctions between users' and providers' viewpoints.

separations of networks, the associated new interests in standards, and the competitive postures of communications service providers and equipment developers and suppliers, are all factors that cause the need for NM and the way in which it is accomplished to take on an increasingly important and changing role. Considerations pertaining to standards for NM are discussed next.

3.1.4 Standards for Network Management

Network management standards include all of the standards making processes and players described in the previous section. Network management programs in standards organizations range from active participation in the basic network management standards process, to development of IAs, development of prototype implementations of network management systems, testing implementations, and various combinations of these activities.

We discuss various perceptions of network management in Section 2 and present the definition that we believe is most appropriate. But, it helps establish the context for standards for network management to briefly mention here some of the differences in perception. Network management, as commonly used in the telephone industry, has been concerned with the management of network elements such as transmission facilities, multiplexers, and switches. Most terminals are operated over analog, circuit-switched networks. Network management, as commonly used in the information processing industry, is primarily concerned with communication between peer-to-peer protocols of multilevel network architectures involving the transmission of digital packets of data.

Developments over the past decade have tended to merge these two basic NM concepts. These developments have included the proliferation of computing networks with distributed processors and the use of processors in telecommunications networks for switching, multiplexing, and for adding a variety of enhanced services to the plain old telephone service. The digitization of telephony and information processing networks coupled with the integration of the services they provide has blurred the distinction between the two and combined them into information networks. Businesses argue that rapid, efficient, and reliable access to information is crucial in the competitive world of industry today. This rapid, efficient, and reliable access requires network management.

So we see that the term "network management" has been used in a variety of ways by different groups to describe a variety of activities. Most of these activities have been associated with enhancing network performance (e.g., reduce blocking and delay) and improving efficiency (e.g., traffic flow control) under abnormal conditions such as unusual traffic patterns, equipment failures, or major outages. The ultimate objective of network management has been to complete as many calls or data transfers as possible over existing facilities even under stress conditions. This required a constant surveillance and the necessary control activities to maintain the network at an optimum performance level and protect essential services during abnormal situations. At the same time, NM has been expected to satisfy users' market needs and maximize returns on investments for both users and service providers. The domains where NM standards are needed are shown in Figure 19. Both public and private domains are indicated.

A key benefit of any telecommunications standard is to promote the creation of a compatible multi-vendor environment. Network management standards also are needed to manage this environment. These NM standards take on added complexity when large networks cross the administrative and domain boundaries indicated in the figure. The desire for customer control capabilities present additional technical and administrative problems.

We describe a number of the standards organizations, with emphasis on NM, in Appendix A. Descriptions of national, international, and government organizations, and how these organizations interact with each other are included. The status of network management activities in these various working groups and subcommittees is described in the following subsection.

3.2 Current Network Management Activities

As discussed earlier, network management is a term used to describe a variety of activities associated with improving network traffic flow, network configuration, and customer service. When abnormal conditions such as unusual traffic patterns or equipment failures occur, the network management process is designed to alleviate congestion or at least reduce network inefficiencies. Network management activities include application of appropriate network controls (e.g., rerouting when necessary), monitoring performance, and providing means to minimize network overloads. At the same time, the network management of commercial carriers should meet customer needs and maximize revenues derived from network services. System objectives include increased call completions, better customer service, protection of essential services, and a higher return on investment.

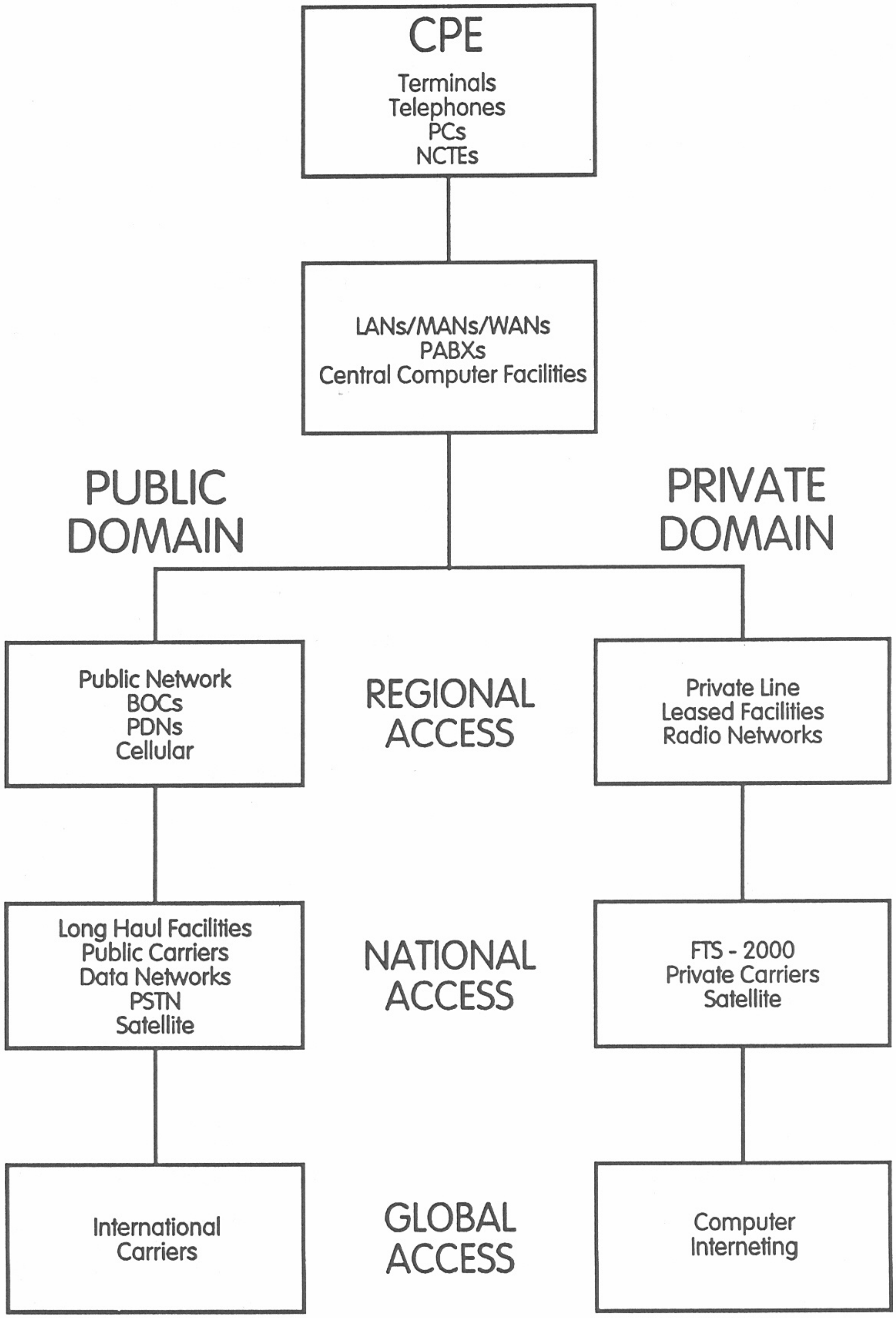


Figure 19. Domains of network management and administrative responsibilities.

In the following subsections, we describe the activities of some of the major organizations that are developing network management standards.

Traditional NM standards for use in the telecommunications industry are concerned with the interaction of network elements such as switches, multiplexors, modems, and transmission channels. International standards for managing traditional network architectures are developed by the CCITT. Managing open system network architectures, on the other hand, is being addressed by Working Group 4 of the ISO/IEC Joint Technical Committee I (JTC1) Subcommittee 21. This subcommittee is formulating a set of functional requirements for the management of services and protocols of the seven layers of "open system" networks. Management standards for computing systems based on the OSI model are directly concerned with the management of the communication aspects of OSI systems.

At the same time, other national organizations are developing network management standards for various network domains: NIST, in the government sector, with the proposed Government Network Management Protocol (GNMP) for managing networks using GOSIP, the IEEE for LAN Management, the Accredited Standards Committee T1 for extending OSI management concepts to a more general structure that includes telephony, and the IAB for the Internet—a collection of 1,000 packet-switched networks, mainly in the United States.

These NM standards activities are described in detail in the following sections. We have divided these activities into three categories of organizations: international, national, and government. The reader is referred to Figures A-1 and A-14 in Appendix A to see how these organizations interrelate.

3.2.1 International Network Management Activities

We include in this group the CCITT, IFIP, JTC1, and the OSI/NM Forum.

International Telegraph and Telephone Consultative Committee (CCITT) Activities

The CCITT’s blue books (CCITT, 1989c) published after the ninth plenary assembly in November 1988, contain several recommendations that are concerned with network management. For example, Volume II, Recommendations E.401-E.880 deal with quality of service, network management, and traffic engineering (Study Group II). Volume III covers ISDN interfaces and maintenance principals in Recommendations I.500-I.600 (Study Group XVIII). Volume IV addresses general maintenance principals with Recommendations M.10-M.787 (Study Group IV). Volume VI covers user-network management in Recommendations Q.930-Q.940 (Study Group XI), and Volume VIII addresses internetwork management with Recommendations X.300-X.370 (Study Group VII). The work of these study groups is continuing during the current plenary session (1988-1992). The Questions dealing with network management that are addressed to each group are summarized in Table 6, and pertinent work is described below.

Recommendation M.30 concerning principals for a Telecommunications Management Network (TMN) is of particular interest here. This Recommendation is given in Blue Book Volume IV.I (CCITT, 1989d) that covers general maintenance principals. Recommendation M.30 presents the general principals for planning, operating, and maintaining a TMN. The TMN provides not only management functions to the network but offers communications support to manage the network.

Figure 20 shows the relationship between the TMN and a telecommunications network that it manages. Functionally, the TMN provides the means to transport and process information that relates to network management.

A generalized TMN physical architecture is shown in Figure 21. The Operations Systems (OSs) processes telecommunication management information to support and/or control various telecommunication management functions. The Data Communications Network (DCN) provides the means for data communication to transport information related to telecommunications management between function blocks. The Mediation Devices (MDs) are stand-alone devices that act on information passing between Network Elements (NEs) and OSs to provide communication control, protocol conversion and data handling, communication of primitive functions, processes involving decision making, and data storage. The Local Communication Network (LCN) is a communication network that supports the data communication functions. Workstations and other Network Elements are connected to each of these functional devices through appropriate interfaces (Q, F, and X) that provide flexibility in making connections for implementing this architecture.

Table 6. CCITT Questions (and Associated Study Groups) Concerned with Network Management

Study Group	Question Number (1988-1992 Plenary Period)
II Telephone Operations	9. International Network Management
IV Transmission Maintenance	23. Telecommunications Management Networks
VII Data Communication	24. OSI Management
XI Telephone Switching and Signaling	2, 3, 6, 13, 24, 25. On AO&M Signaling Architectures
XV Transmission Systems	9. AO&M interfaces
XVII Data Communications Over Telephone Circuits	9. Network Management
XVIII Digital Networks	14. ISDN Operations and Maintenance

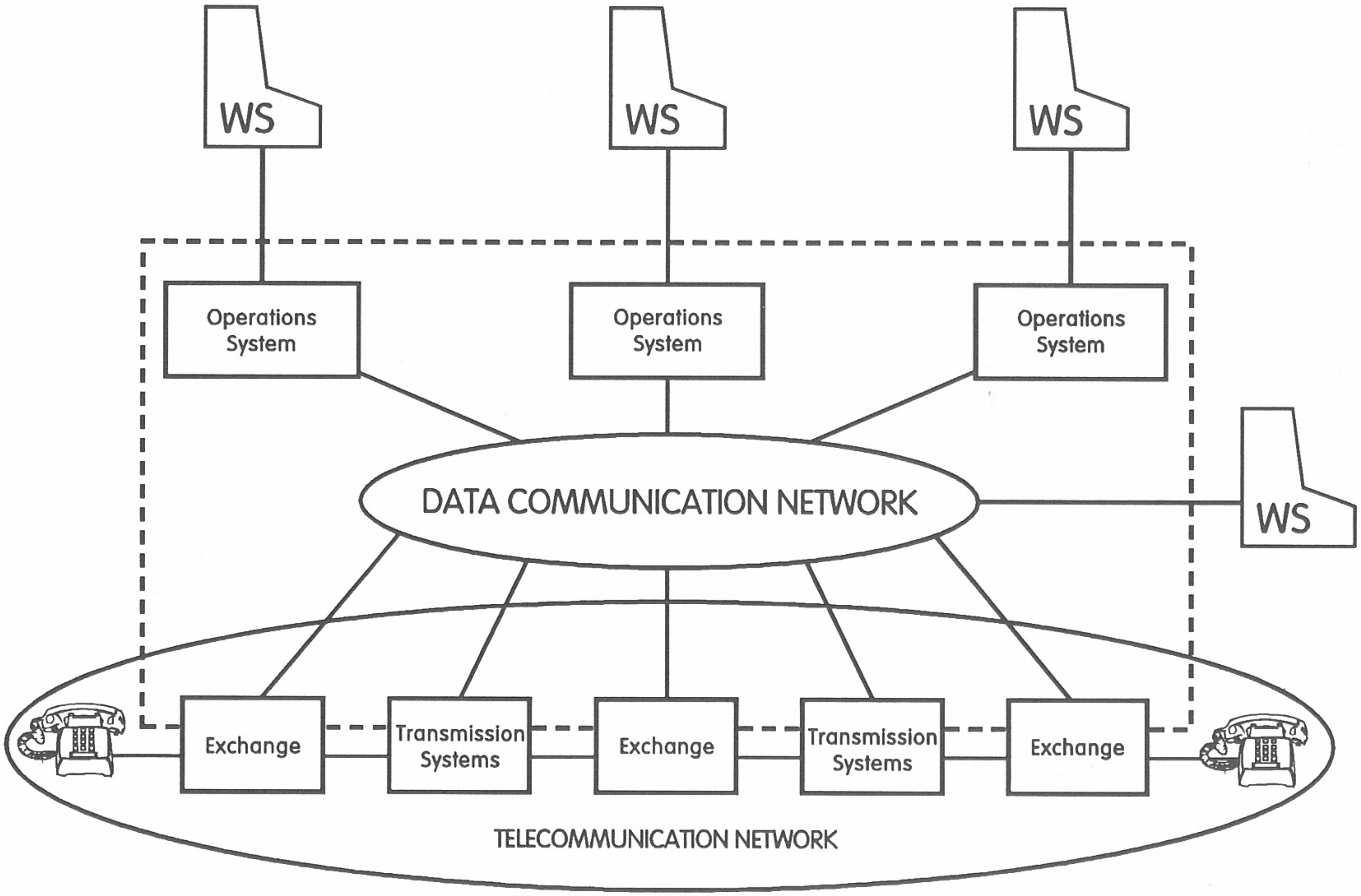


Figure 20. Relationship of TMN to a telecommunications network (CCITT, 1989d).

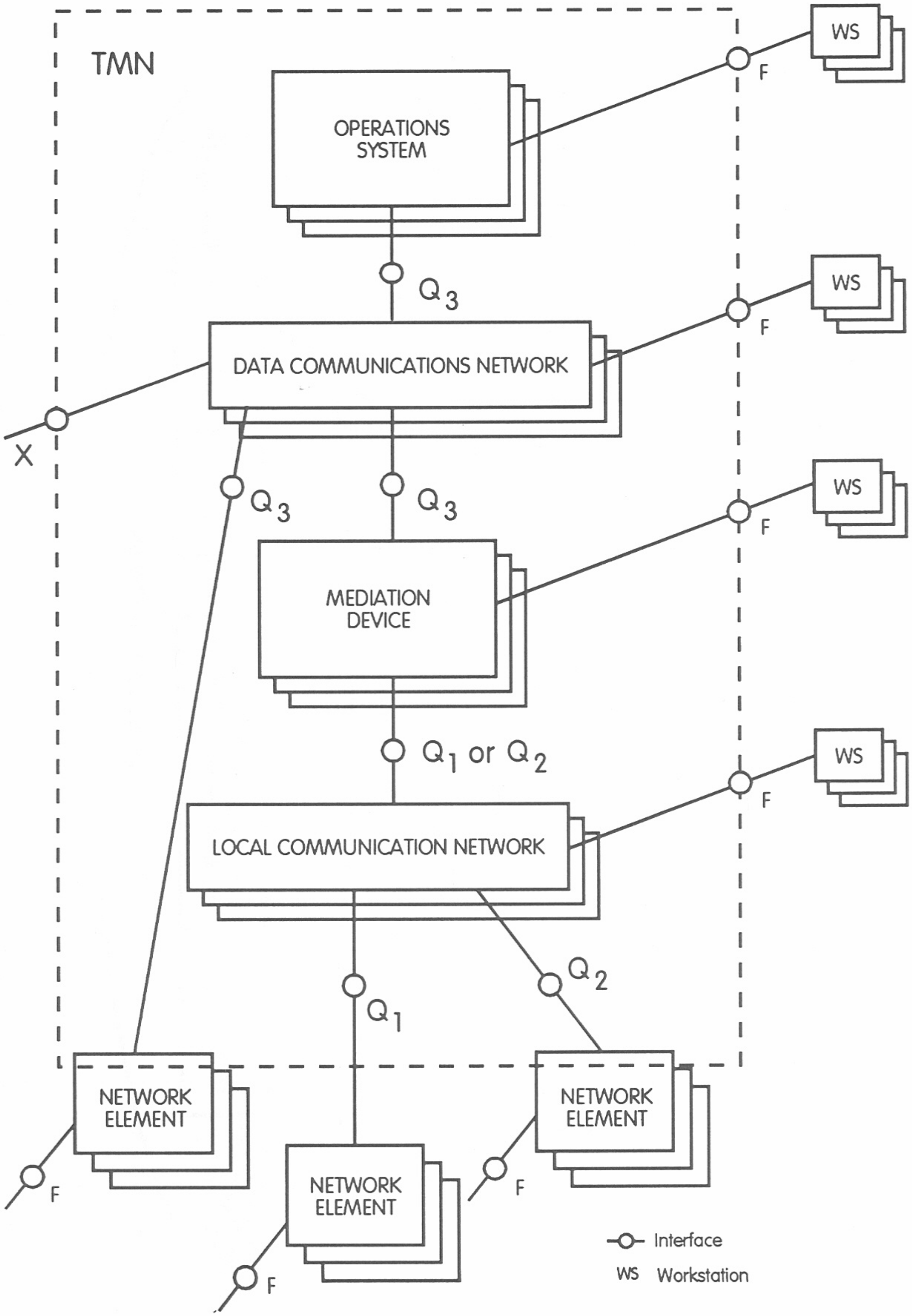


Figure 21. Physical TMN architecture (CCITT, 1989d).

Two types of functions performed by a TMN are defined below.

General Functions

- Transport — provides for the movement of information among TMN elements
- Storage — provides for holding information over controlled amounts of time
- Security — provides control over access for reading or changing information
- Retrieval — provides access to information
- Processing — provides for analysis and information manipulation
- User terminal support — provides for input/output (I/O) of information.

Application Functions

- Performance management
- Fault (or maintenance) management
- Configuration management
- Accounting management
- Security management.

The CCITT (1989b), recognizing that a number of events can lead to serious congestion of the international telephone service, has also developed a series of Recommendations (E.410-E.414) that addresses this problem. Recommendation E.410 defines International Network Management (INM) as "the function of supervising the international network and taking action when necessary to control the flow of traffic. Network management requires real-time monitoring and measurement of current network status and performance, and the ability to take prompt action to control the flow of traffic". EAIO goes on to state, "The objective of network management is to enable as many calls as possible to be successfully completed. This objective is met by maximizing the use of all available equipment and facilities." Network management functions that identify adverse conditions and minimize their impact include the following:

a) monitoring the status and performance of the network on a real-time basis, which includes collecting and analyzing relevant data

b) detecting abnormal network conditions

c) investigating and identifying the reasons for abnormal network conditions

d) initiating corrective action and/or control

e) cooperating and coordinating actions with other network management centers, both domestic and international, on matters concerned with international network management and service restoration

f) cooperating and coordinating with other work areas (e.g., maintenance, operator services, or planning) on matters that affect service

g) issuing reports of abnormal network situations, actions taken, and results obtained to higher authority and other involved departments and Administrations, as required

h) providing advance planning for known or predictable network situations.

Recommendation E.411 provides operational guidance for network management, including

- status and performance parameters
- expansive and protective traffic controls
- criteria for application of controls.

Recommendation E.412 provides the following information on network management controls:

- traffic to be controlled
- exchange controls
- automatic controls
- status of controls
- operator controls.

Recommendation E.413 provides guidance on planning for events such as

- peak calling days
- failures of transmission systems
- failures of exchanges
- failures of common channel signalling systems
- mass-calling situations
- disasters
- introduction of new services.

Recommendation E.414 provides guidance on the functional elements of a network management organization which need to be identified internationally as contact points. These comprise

- planning and liaison
- implementation and control
- development.

Effective network management requires communications and cooperation between various international network management centers. This includes the exchange of real-time information regarding network status and performance of the national networks involved. This includes switch status and traffic flow in coverage locations. This can involve substantial exchanges of data on a regular basis. These large data exchanges may be supported by the TMN (Recommendation M30) discussed previously. Smaller data exchanges may be handled by telex, facsimile, or by the signaling system itself.

International Federation for Information Processing (IFIP) Activities

Working Group 6.6 of the IFIP is concerned with network management. This group has developed a Users Requirements document that includes list, concepts, and definitions at a high level. Work includes a network model to identify what is needed to accommodate the user requirements that have been identified. The aim is to show what information is needed and what controls are required for network management. Work is being done in the context of layered protocols such as OSI. Results will be given to individuals and organizations and are expected to lead to protocols and standards for network management.

Joint Technical Committee 1 (JTC1) Activities

The JTC1, Subcommittee 21, Working Group 4 and the CCITT Study Group VII are jointly responsible for the development of Recommendations and International Standards for OSI management, the services, protocols, and functions that are used for Systems Management, and the Structure of Management Information (SMI). (A summarized description of the layered architectural model that has been standardized by the ISO and that is followed in developing these standards is included in Appendix B.) Other groups are responsible for development of standards and recommendations for the management aspects of particular layers of the OSI reference model including layer management protocols, management aspects of (N)-layer operation, and managed objects visible to system management.

OSI management standards developed to date by the JTC1 subcommittee 21 are listed in Appendix C. They define the facilities to control, coordinate, and monitor the resources which permit communications in an OSI environment.

The OSI management framework (ISO/IEC, 1989) defines five specific functional areas of network management. The functional areas and their functions (not necessarily exhaustive) are

> **Fault Management** which enables the detection, isolation, and correction of abnormal operation of the network and its environment. Fault management includes functions to
>
> a) maintain and examine error logs
> b) accept and act upon error detection notifications
> c) trace and identify faults
> d) carry out sequences of diagnostic tests
> e) correct faults.
>
> **Accounting Management** which enables the use of the network to be measured and costs for such use to be determined. Accounting management includes functions to

a) inform users of costs incurred or resources consumed
b) enable accounting limits to be set and tariff schedules to be associated with the use of resources
c) enable costs to be combined where multiple resources are invoked to achieve a given communication objective.

Configuration Management which identifies, exercises control over, collects data from, and provides data to network elements for the purpose of preparing for, initializing, starting, providing for continuous operation of, and terminating interconnection services. Configuration management includes functions to

a) set the parameters that control the routine operation of the network
b) associate names with managed objects and sets of managed objects
c) initialize and close down managed objects
d) collect information on demand about the current condition of the network
e) obtain announcements of significant changes in the condition of the network
f) change the configuration of the network.

Performance Management which enables the behavior of resources and the effectiveness of communication activities to be evaluated. Performance management includes functions to

a) gather statistical information
b) maintain and examine logs of network state histories
c) determine network performance under natural and artificial conditions
d) alter network modes of operation for the purpose of conducting performance management activities.

Security Management which supports the application of security policies. Security management includes functions to

a) create, delete, and control security services and mechanisms
b) distribute security-relevant information
c) report security-relevant events.

An architectural model for the OSI seven-layer protocols that participate in OSI management is shown in Figure 22. The management structure illustrated could apply to other layered architectures as defined in Appendix D. Management is accomplished by means of functions provided by systems management, (N)-layer management, and (N)-layer protocol operations.

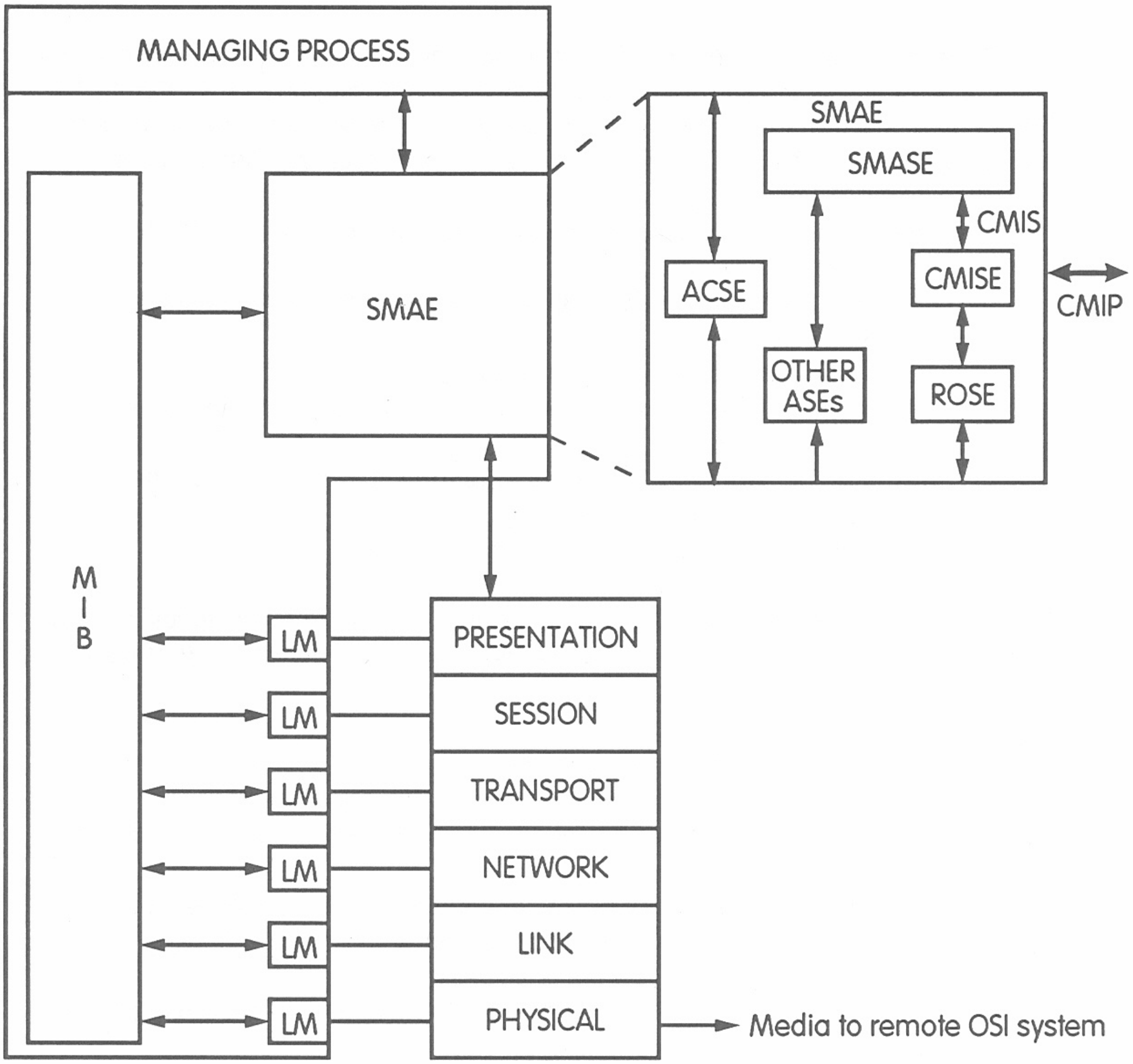


Figure 22. Architectural model of OSI management (Bartee, 1989).

Examples of systems management functions are functions that involve multiple layers or are layer independent. (N)-layer management functions are functions required to assure integrity of layer protocols. Such functions may allow changing layer parameters to accommodate changing environmental conditions or user needs. The (N)-layer protocol operations provides management functions required to agree on parameter sets for local communications.

In the OSI model of Figure 22, a system management applications entity (SMAE) is responsible for communications (Bartee, 1989). Layer management modules (LMs) provide access to managed objects associated with each protocol layer. The MIB contains information for each protocol entity and for the entire system. The SMAE consists of the association control service element (ACSE), the systems management application service element (SMASE), and the common management information service element (CMISE). The CMISE services are used to manipulate data contained in the MIB. The MIB contains information about managed objects. Entries in the MIB, listing the attributes and associated values for each object, are arranged hierarchically into a Management Information Tree (MIT). The basic network management framework is shown in Figure 23. Managed objects are also characterized by the operations that can be performed on them and the actions they can emit to the manager system. The common management information protocol specifies protocols for exchanging this information between OSI systems and between managers and devices.

The OSI management standards, while currently at an intermediate stage of their development, are maturing rapidly. The ultimate goal of these standards is to enable the development of interoperable, multi-vendor products for the management of computer and communications systems and networks. Key areas of management standardization are architecture, protocols, system management functions, and the SMI. The Common Management Information Services and Protocol standards, CMIS and CMIP, have now become International Standards. Many other needed management standards are still at the Draft International Standard (DIS) status. However, these DISs, available at the beginning of 1991, compose a subset of management standards that make it possible for vendors to build useful systems to meet some immediate network management requirements. Still other standards are planned or proposed (for example, the Software Management Function and the Generic Managed Objects Standards), but these have not yet been added to the ISO schedule for standardization.

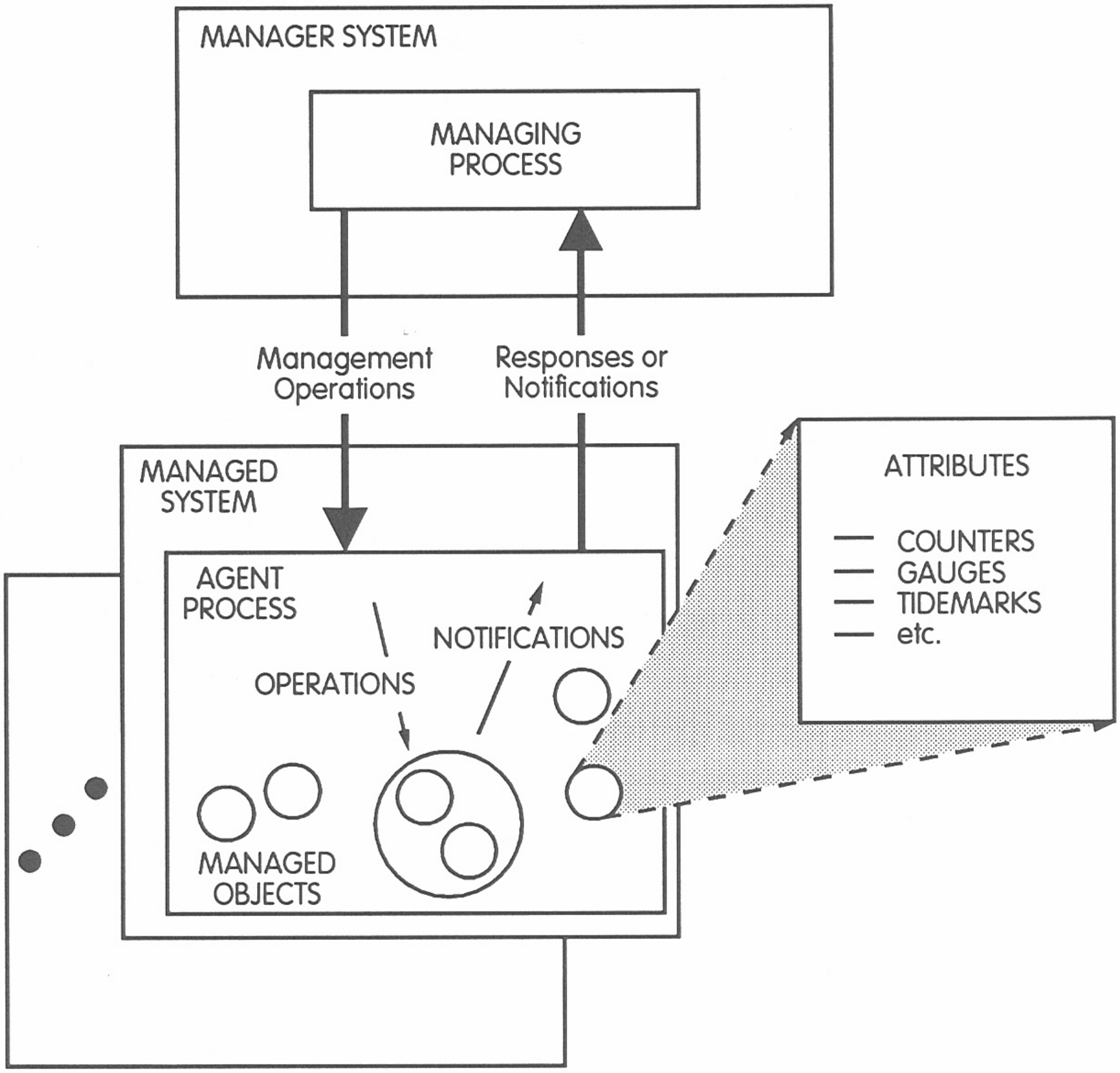


Figure 23. Basic network management framework (Bartee, 1989).

OSI/NM Forum Activities

The OSI/NM Forum is an international consortium of information network equipment vendors, service providers, and users working to accelerate the development and use of OSI standards. A key objective is to achieve and demonstrate multivendor network management interoperability.

In October 1991, the OSI/NM Forum released specifications for a complete implementation of the interface for the exchange of network management information (OSI/NM Forum, 1990). A summary of these specifications consisting of ten documents is given in Table 7.

These specifications use CMIP/CMIS and apply to any type of information processing system or communications network including voice or data, local area or wide area, proprietary or standards based. The real purpose is to provide a total marriage of network resources on an end-to-end basis since it allows different vendors' management systems to interoperate.

Conformance testing for Release #1 compliance is essential. The Corporation for Open Systems in the United States and the Standards Promotion and Application Group in Europe have developed test software and procedures in conjunction with the Forum. The software is designed to test the transport layer, CMIP, and implementations of managed objects and messages. Conformance test reports (CTRs) will be used to characterize a product. Matching CTRs should insure compatibility of two products (Warner, 1991).

Some differences between the Forum objective and the work of the ISO and CCITT are noteworthy. The ISO and CCITT are defining management standards that focus on managing particular kinds of networks. The OSI/NM Forum is attempting to apply those standards to the management of any network. For a summary of the architecture and key concepts that have been adopted by the forum for interoperable network management see Embry et al. (1991).

3.2.2 National Network Management Activities

Network management standards for the United States are being developed primarily by three major groups accredited by ANSI. They are the IEEE Committee on Network Operations and Management (IEEE/CNOM) for LANs, the Accredited Standards Committee for Telecommunications (ASC T1) for telephone networks and ISDN, and the Accredited Standards Committee for Information Processing Systems (ASC X3). The subcommittees within each of

Table 7. OSI/Network Management Forum Release #1* Specifications
(Dated October 12, 1990)

Forum 001
Protocol Specification - Issue 1

Specifies the elements of the OSI/NM Forum interoperable interface protocols. Designed to facilitate communication between equipment of different vendors, using either connection-oriented WAN or connectionless LAN lower layers. Based on international standards, including CMIS and CMIP, plus agreements reached regionally in defining implementation profiles.

Addendum to Issue 1

Includes Protocol Implementation Conformance Statements (PICS) and errata to Issue 1. PICS, designed for use by conformance testers, lists the features of each protocol, the base standard requirement for each, the Forum requirement for each, and any Forum constraints. PICS proforma are in tabular form, for completion by the developer to indicate which options and capabilities have been implemented.

Forum 002
Application Services - Issue 1.1

Specifies common management services to support the initial functional areas undertaken by the Forum: 1) generic event management, 2) alarm management, and 3) object and attribute management. In addition to a number of generic models, defines protocol and procedures to enable Conformant Management Entities (CMEs) to transmit network management functional data. Includes SMASE Implementation Conformance Statements (SICS), in tabular format, designed for use in conformance testing.

Forum 003
Objective Specification Framework - Issue 1

Provides guidelines and a notation for defining managed object classes, attributes, name bindings, notifications and operations. Intended for use by designers in developing object specifications for the Forum library.

* This release consists of ten documents which together specify a complete implementation of the Forums interoperable interface for the exchange of network management information.

Table 7. continued

Forum 004
Forum Architecture - Issue 1

Identifies major system components such as: the interoperable interface, Conformant Management Entity, Management Network (MN). Management Solution (MS), and Managed Elements (MEs). Presents interoperable network management as a general model, viewed from several perspectives, each of which describes a different abstraction of specific aspects of the general model, its major components and their interactions. Because other Forum documents reference the concepts contained in the Forum Architecture, this document is recommended "first reading" for new readers of Forum documentation.

Forum 005
Forum Glossary - Issue 1

Provides short definitions of key terms and provides references to other Forum documents where terms are completely defined and used in context.

Forum 006
Forum Library of Managed Object Classes, Name Bindings and Attributes - Issue 1.1

The source for the definitions of managed object classes, name bindings and attributes. These definitions are based on the guidelines specified in the Forum Object Specification Framework (Forum 003). To aid in conformance testing, Object Implementation Conformance Statements (OICS) are also included in tabular form, to be used by developers to specify which options and capabilities have been implemented.

Forum 007
Managed Object Naming and Addressing - Issue 1

Provides requirements for the naming and addressing of managed object instances. Extends and supercedes the naming sections found in the Forum Object specification Framework (Forum 003) and the Forum Architecture (Forum 004), and is reflected in the Forum Library of Managed Object Classes, Name Bindings and Attributes (Forum 006).

Table 7. continued

Forum 008
Forum Release 1 Conformance Requirements - Issue 1

Provides a summary of Network Management product conformance-related requirements, such that developers can understand what is required to pass conformance tests.

Forum 009
Shared Management Knowledge - Issue 1

Provides the means whereby Conformant Management Entities can achieve a common understanding of each other’s management protocols, procedures and capabilities to exchange management information.

these organizations that are involved with network management are listed in Figure 24. The NM activities being conducted in each group are described in the following paragraphs.

ASC X3 Activities

Accredited Standards Committee X3 develops standards in the general areas of computer information-processing systems and office systems. Work includes standardization of computer systems and subsystems to provide for interoperability of hardware and portability of software. The X3 committee also participates in the development of international standards in these areas. Most of the network management activities are conducted by technical committees X3S3 for data communications, X3T5 for open systems interconnection, and X3T9 for the Fiber Digital Data Interface (FDDI). The work of these committees and subcommittees is briefly described below.

The long-term objective of X3T5.4 is to produce a comprehensive set of OSI Management standards for the OSI networking environment. Implicit in this goal is that X3T5.4 will work concurrently with ISO/IEC JTC1 SC21 WG4 to develop the content of the standards, and will provide leadership, guidance and input to WG4 for the standards development process.

The strategy of this group is to use a two phased approach: Phase 1 — included OSI management framework, system management overview, CMIS/P, configuration management, fault management, and definition of conformance. Phase 2 — will include completion of a comprehensive set of OSI Network Management standards.

Technical Subcommittee X3T5.5 is dealing with layer management in the OSI upper layers. This work is applicable to user groups wishing to provide management services and functions in accordance with the basic reference model of OSI.

Goals of the project are to define and specify management information related to the operation of the Session, Presentation, and Application layers. This information consists of layer managed-objects to be acted upon by systems management for the purpose of performing the functions of Fault Management, Performance Management, Accounting Management, etc.

The program of work will proceed to develop layer-specific management standards for the upper three layers of OSI. The work will be done within X3T5.5 in the United States, and ISO/IEC JTC1/SC 21/WG6 internationally. Close liaison and collaboration needs to be maintained with the relevant activities of X3T5.4 and ISO/IEC JTC1/SC 21/WG4.

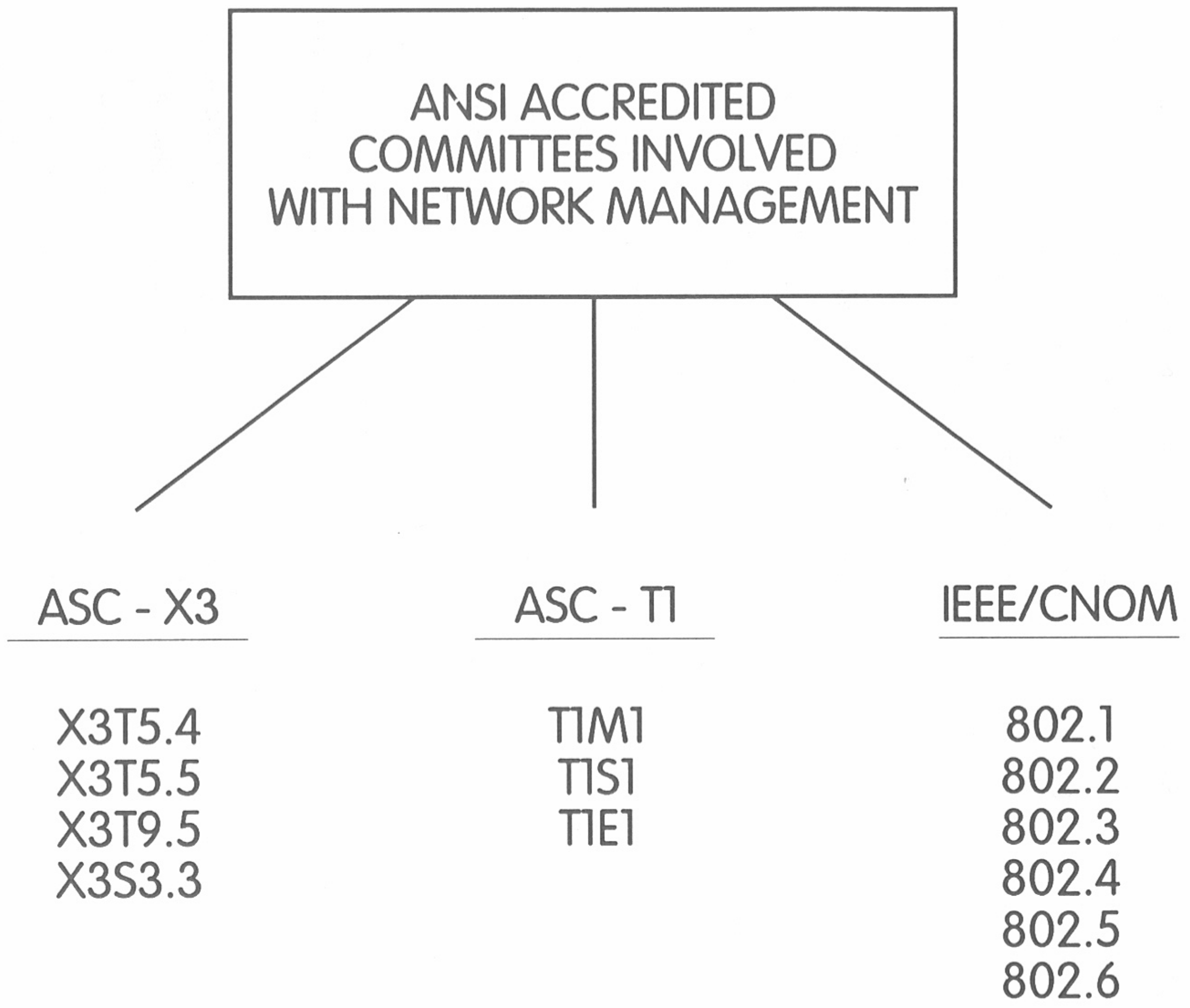


Figure 24. ANSI accredited standards committees involved with network management (as of April, 1992).

There are two network management standards development projects within X3S3.3 for an "OSI Network Layer Management Information Specification" and an "OSI Transport Layer Management Information Specification." The purpose of these projects is to develop a complete specification of Network and Transport layer management information, i.e., the abstract syntax and semantics of the information contained within the OSI Management Information Base that is directly related to the Network and Transport Layers.

ASC T1 Activities

Activities of the subcommittees of T1 are described below. The T1M1 Subcommittee deals with network management activities by applying the principals of OSI management to the interface specification of Telecommunications Management Networks. Their mission is to develop internetwork operations, administration, maintenance and provisioning standards, and technical reports to interfaces for U.S. telecommunications networks; some of which are associated with other North American telecommunications networks. These standards may apply to planning, engineering and provisioning of network resources; to operations, maintenance or administration process; or to requirements and recommendations for support systems and equipment that may be used for these functions. This subcommittee also will develop positions on related subjects under consideration in other domestic international standards bodies.

The technical subcommittee covers standards and reports for internetwork planning and engineering functions such as traffic routine plans; measurements and forecasts; trunk group planning; circuit and facility ordering; network tones and announcements; location, circuit, equipment identification and other codes; and numbering plans. The T1M1 also considers standards and reports for all aspects of internetwork operations such as network management; circuit and facility installation, line-up, restoration, routine maintenance, fault location and repair; contact points for internetwork operations; and service evaluation. The work of the Technical Subcommittee includes standards and reports regarding test equipment and operations support systems together with the required network access and operator interfaces. Further, the Technical Subcommittee is concerned with administrative support functions such as methods for charging, accounting and billing data. Of necessity, the scope of this work requires a close and coordinated working liaison with other T1 Technical Subcommittees as well as external standard-setting bodies.

Although T1M1.5 has the primary role in network management, work is also going on in T1S1 and T1E1 with parts of ISDN Access Management and in T1S1 with CCS Management. These three subcommittees (T1M1, T1S1, and T1E1) correspond with CCITT work on management in Study Groups II, IV, VII, XI, XV, XVII, and XVIII.

A technical report prepared by T1M1.5 presents a methodology for developing services and protocols for TMN applications (ANSI, 1990). This methodology is intended to provide a uniform set of interface specifications for the TMN regardless of technology. Thus, concepts for both communications and computing disciplines are integrated taking into account the standard representations in this area within the CCITT and the ISO.

The TMN architecture is described in ANSI (1989c). Protocols for the lower layers 1-4 and upper layers 5-7 are given in ANSI T1.204 and ANSI T1.208, respectively (ANSI, 1989a and 1989b). The generic network model for developing certain standards is given in T1.214 (ANSI, 1989d).

IEEE/CNOM Activities

This recently-formed committee deals with matters in the area of network management for LANS. The charter of CNOM is to provide a focus within the IEEE Communication Society for those interested in network operations. Operations include all actions required to plan, engineer, provision, install and maintain, administer and manage the communications network. LAN standards that have been developed by the IEEE include several which are expected to evolve into ISO standards.

The IEEE 802.1 working group recently issued two LAN/MAN network management protocols and guidelines (IEEE, 1990a and 1990b). The management protocol is similar to the Common Management Protocol over TCP/IP (CMOT) for Internet. IEEE 802.1 provides an overview to the family of 802 standards, describes the relationship of IEEE 802 work to the OSI Basic Reference Model, and explains the relationship of these standards to higher layer protocols. Standard 802.lB specifies an architecture and protocol for the management of IEEE 802 LANs, which are used independently of the layer or layers being managed. Specifications for layer-specific manageable objects are covered by other IEEE projects, i.e., 802.2, 802.3, 802.4, and 802.5. All of these are in various phases of completion and are targeted for ISO standards.

3.2.3 Government Network Management Activities

This section could include activities of the NIST National Computer Systems Laboratory (NCSL), National Telecommunications and Information Administration (NTIA), the Federal Telecommunications Standards Committee (FTSC), Defense Information Systems Agency's (DISA) Center for Standards, and the IAB. However, only the NCSL and IAB activities are included here. See Appendix A for discussion of NTIA, FTSC, and DISA activities.

NIST/NCSL Activities

The Systems and Network Architecture Division of NCSL conducts work to advance the development and implementation of OSI technology. The NIST/OSI workshop, established by NCSL in 1983, is an open international forum that focuses on OSI layer problems such as electronic mail, file transfer, security, directory services, and network management. In the latter area, the emphasis is on integrated, interoperable network management as described below.

As the success of OSI creates large, multi-vendor networks composed of many components, the management of network functions and the protection of information transmitted through networks becomes more challenging. Proprietary systems provide for these functions but multi-vendor open systems have different requirements. NIST Special Publication 500-175 (Aronoff et al., 1989), *Management of Networks Based on Open Systems Interconnection (OSI) Standards: Functional Requirements and Analysis,* examines current and proposed network management systems to determine both user and functional requirements for network management. The examination of requirements focuses on those necessary for interoperability in the following broad areas: architecture, configuration management, fault management, security management, performance management, and accounting management.

To assist federal agencies in implementing Federal Information Processing Standard (FIPS) 146 (GOSIP), NCSL and the General Services Administration (GSA) collaborated in 1991 in the pilot deployment of X.500 on Federal Telephone System (FTS) 2000, the government-wide telecommunications network. The pilot project transfers a key technology, the OSI Directory, to government agencies to support naming, locating, and addressing resources and provides experience in large-scale deployments of X.500 to the federal community.

To meet the need for interoperable network management products within the government, NCSL is developing a FIPS for Network Management to be called the Government Network

Management Profile (NIST, 1991). Phase 1 GNMP, proposed in January 1991, consists of specifications pertaining to management communications, management information, and systems management functions. Each subsequent phase will add to the management capabilities and managed objects proposed in Phase 1 GNMP.

Another important aspect of network management standards activity is the development of IAs. The Network Management Special Interest Group (NMSIG) of the OSI OIW (sponsored by NIST and the IEEE Computer Society) is developing IAs based on the emerging NM standards. These agreements are being developed in phases that align with the ISO standards as they progress from Committee Draft (CD) to International Standard (IS).

It is expected that the administrator of GSA will provide for the procurement of Network Management products according to GNMP (NIST, 1991). The GOSIP is cited in the GNMP to specify the protocol stack upon which management information can be conveyed. The GOSIP also specifies applications, such as File Transfer, Access and Management (FTAM), Message Handling System (MHS), and Virtual Terminal Protocol (VTP), that can be used to support network management applications. Future versions of the GNMP will enable management of more GOSIP components (e.g., transport connections and key exchanges). Future versions of the GOSIP will cite the GNMP to specify the management protocols, services, and information needed to facilitate interoperable multi-vendor management of GOSIP-complaint systems. As both the GNMP and the GOSIP mature, it is expected that they will continue to cross-reference the latest versions of each other.

IAB Activities

The IAB is the coordinating committee for Internet. Internet is a collection of over 1,000 packet switched networks located principally in the United States. The IAB has two principal task forces for managing Internet. They are: 1) the Internet Engineering Task Force (IETF) and 2) the Internet Research Task Force (IRTF). The IETF charter includes responsibility for specifying short and mid-term architecture and protocols and for recommending standards for IAB approval. Within IETF is one technical area entitled network management with several working groups. One NM working group is dealing with the MIB. Another is dealing with the TCP/IP based SNMP to accommodate short-term needs. Another is working on an ISO

CMIS/CMIP framework for the long-term needs of the Internet Community. This later activity is known as CMOT for Common Management Information Services and Protocol over TCP/IP.

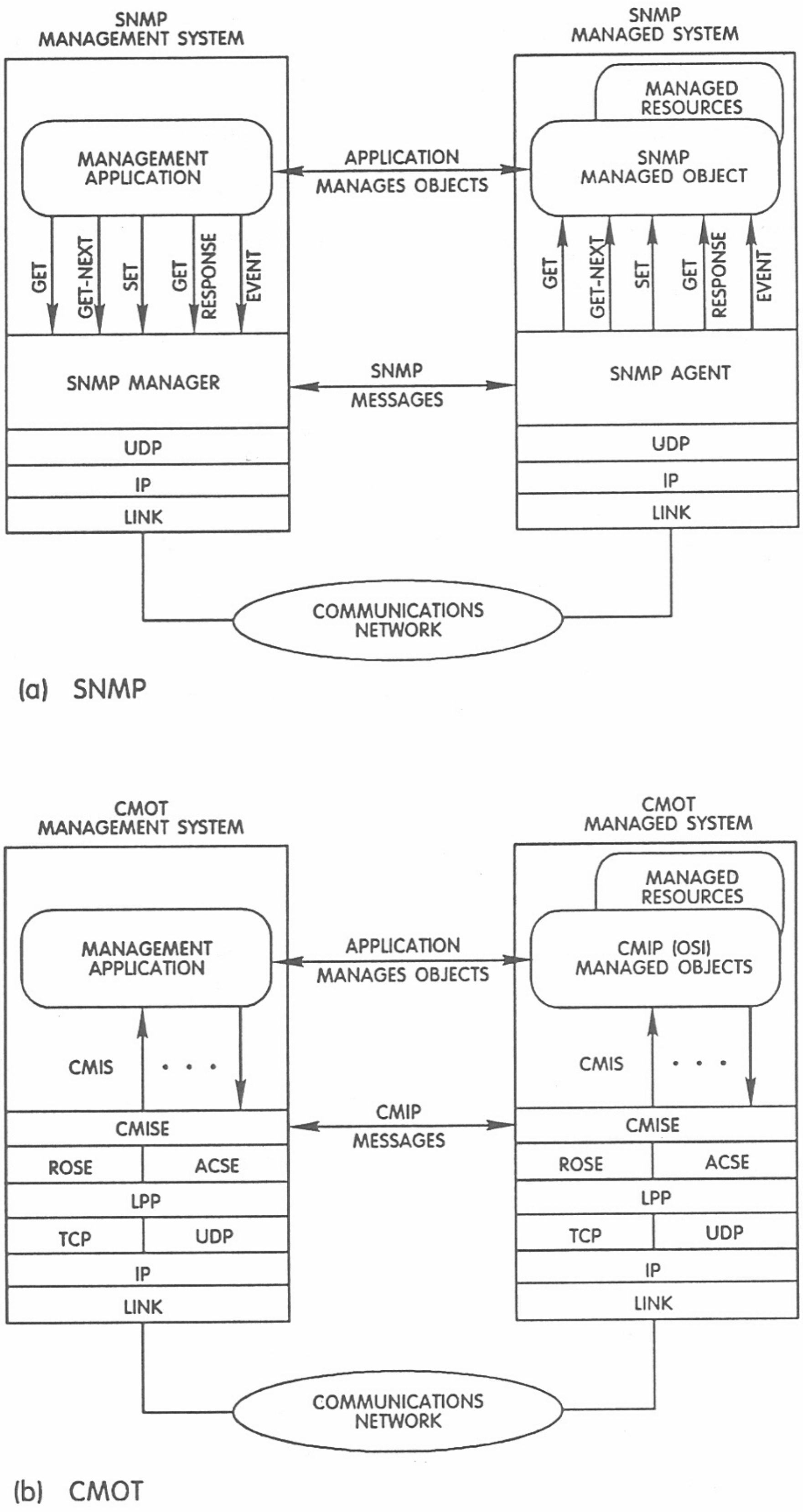
The SNMP standards work is conducted by various groups within the IETF. One group is concerned with IAs for managing asynchronously generated events and another group is concerned with protocol specifications for SNMP security management. The MID working group defines objects and provides standards for management support.

Currently, the SNMP appears to be the de facto standard for managing TCP/IP networks while CMOT is considered the long term solution. SNMP's success is largely due to the fact that it is easy to implement and requires low processing and memory resources. The disadvantages of SNMP are the poor response times in large networks and the excessive time required for retrieving data from managed objects. SNMP is more useful for monitoring networks than for controlling them. Many of the SNMP shortcomings are addressed with CMOT.

The CMOT group known as "OSI Internet Management" (OIM) working group provides CMIP-based management standards for the Internet protocols and OSI LAN/WAN portions of Internet. A Management Services Interface Group (MSI) is defining a common set of services for managing systems in the multivendor environment.

The SNMP and CMOT concepts are described by Ben Artzi et al., (1990) and summarized here using his paper. Figure 25 compares the two architectures. The SNMP architecture in Figure 25a provides applications with a simple set of commands (Get, Set and Get-Next) which are packaged using the Basic Encoding Rules (BER) associated with ISO Abstract Syntax Notation One (ASN.1) and sent over existing UDP/IP (User Datagram Protocol) services. There is also a very limited trap message, which allows six standardized types of unconfirmed events to be reported asynchronously.

Current SNMP implementations are centered around a core set of three specifications: the SNMP protocol over a UDP/IP protocol stack (Case et al., 1989), the rules for SMI (Rose and McCloghrie, 1988) for use with SNMP, and an initial collection of about 100 standardized SNMP objects (McCloghrie and Rose, 1988). The initial set of objects, termed "MIB-I," comprise a MIB that provides for limited fault and configuration management. MIB-I objects represent parameters that relate to TCP/IP protocols, system address tables, interface tables, and system identification information.



(a) SNMP

(b) CMOT

Figure 25. Comparison between SNMP and CMOT concepts (Ben-Artzi et al., 1990).

Figure 25b shows the CMOT architecture. The application services provided by CMOT are defined by Common Management Information Services, the service definition for the ISO CMIP protocol (ISO 9595). As shown in the figure, the application layer is based on OSI and contains Common Management Information Service Element, Remote Operations Service Element (ROSE), and Association Control Service Element. The transport and network layers are TCP/UDP and IP, respectively. The presentation layer consists of a Lightweight Presentation Protocol (LPP), and provides a mechanism for supporting OSI application services directly over TCP/IP environments (Rose, 1988).

3.2.4 Related Activities

A number of activities are being conducted by various groups in network management or closely related to network management that have not been covered previously. Included in this group are the Corporation for Open Systems, the Information Industry Liaison Committee (IILC), and NIST's OSI Implementors Workshop. A summary table of standards activities in network management is included.

COS Activities

The mission of the Corporation for Open Systems is "to provide an international vehicle for accelerating the introduction of interoperable, multi-vendor products and services." A primary function is to develop conformance testing and certification of OSI standards including NM standards. This supports the accelerated deployment of open systems. In performing these functions, COS manages a user-driven requirements process concerned with identifying and coordinating an attack upon barriers to the full deployment of open systems. The COS forum provides for necessary interaction between users, vendors, and service providers and has attracted such diverse user groups as the Manufacturing Automation Protocol/Technical Office Protocol (MAP/TOP) Users Group, the User Alliance for Open Systems (UAOS), and members of the Electrical Power Research Institute (EPRI), and other groups continue to show interest.

The initial leader in providing conformance testing and certification, COS, together with NIST, the American National Standards Institute, the Computer and Business Equipment Manufacturers Association (CBEMA) and other stakeholders, is helping to create and mobilize a national policy for information technology testing and certification. In pursuit of those ends, COS has worked with NIST under a cooperative venture agreement to help create the policies and procedures for GOSIP and has contributed several of the tests and means of testing now found on the GOSIP register. Since no standards for network management are complete, a COS network management subcommittee (NMSC) is trying to expedite standards work on NM and is monitoring the ISO and CCITT to insure that the work is not diverging. COS works closely with the Standards Promotion and Applications Group in Europe and the Promoting Conference for OSI (POSI) in Japan to ensure global harmonization (COS, 1987). COS also maintains ties to the North American ISDN Users Forum (NIU Forum) and the NMF.

IILC Activities

The IILC is a forum in which ONA issues are addressed under a consensus resolution process. Working committees currently are addressing a number of complex issues including, numbering plans for enhanced service providers (ESPs), ONA service uniformity, framework for unbundling services, future network needs, switch call control, and several others. None are considered network management issues but all are indirectly related.

NIST/OIW Activities

The OIW was established by the NCSL of NIST as an open international forum. Participants include manufacturers, vendors, service providers, industry and government users. Objectives are accomplished through special interest groups (SIGs) which focus on certain aspects of the OSI layers and applications including network management. A summary of NIST's network management program is given below. For more detail see Aronoff et al. (1989).

The NIST network management program includes three major activities: development of the implementation agreements, active participation in the basic network management standards process, and research that supports these activities through development of prototype implementations of network management systems.

The focal point of the activity to develop suitable IAs is the NIST OIW. Approved IAs for OSI do not lead directly to interoperable implementations in multi-vendor products. The typical IA contains a number of incompatible subsets and options that hinder interoperability. To achieve interoperable commercial products, the NIST established an open forum in 1983 where implementors and users of OSI products could meet to reach specific agreements concerning the protocols, subsets, and options to be implemented. The output of these workshops is a documented set of agreements that point the way to implement interoperable OSI products. Several groups have adopted the workshop output as the basis for functional profiles, including General Motors for MAP, Boeing Computer Services for TOP, and the U.S. Government for GOSIP. In addition, the Corporation for Open Systems uses the workshop output as the basis for conformance testing profiles.

Other Organization's Activities

Table 8 presents a list of organizations involved with OSI network management standards. This list, taken from Aronoff et al. (1989), may be somewhat out of date in terms of the status column, but it does indicate the extent of recent activities in network management. Some tables have been completed but new ones are continuously being added and addressed.

4. NETWORK MANAGEMENT PRODUCTS

The purpose of this section is to examine the broad spectrum of network management products available and the scope of those products in managing today's diverse network environment. Network management products are discussed within the context of three management domains-transport, data, and voice-defined in Section 4.1. Section 4, in total, addresses the functionality of network management products applied within each of these domains and across domains at the physical level of network management. Deliberately, an attempt to represent all products and vendors dealing with network management has not been made. A vendor or product is identified only as a typical representation of the functionality being discussed and as an efficient and effective method for developing and presenting that discussion.

Products available for management of a network are as diverse as the network itself. While diverse voice and data networks are being consolidated into uniform, comprehensive networks and integration is occurring across network services, management across network components and services is not keeping pace.

A wide variety of products or tools of various levels of functionality are available for use in managing the telecommunication networks. Management tools span a range from managing a single vendor-specific network element to management of enterprise-wide (see Section 4.1),