NTIA Report 93-295

Network Management: A Review of Emerging Concepts, Standards, and Products

R.D. Jennings
R.F. Linfield
M.D. Meister

U.S. DEPARTMENT OF COMMERCE
Ronald H. Brown, Secretary

Thomas J. Sugrue, Acting Assistant Secretary
for Communications and Information

April 1993

PREFACE

The Institute for Telecommunication Sciences (ITS) is performing a series of projects concerned with the roles of advanced communication satellites in Integrated Services Digital Networks (ISDN) and the use of advanced satellite system technology to enhance rapid restoration of services provided by the Public Switched Network (PSN) following a natural or "manmade" disaster. Goals of the work are (1) to promote an effective integration of advanced satellite systems with the developing terrestrial broadband networks, (2) to perform studies that examine uses of advanced communication satellite systems to reduce national vulnerability to telecommunication outages, and (3) to identify needs and recommend interface and functional standards required for integrated services, such as ISDN, in a terrestrial-satellite broadband transmission and switching environment.

The purpose of the project addressed in this report has been to present a conceptual development of the technology termed network management, to describe the many organizations that are actively involved with the development of network management standards, to examine the functional characteristics of a variety of network management products, and to discuss some of the important issues and trends that are creating new requirements for network management. Interest in network management technology and some initial support for this work have been provided by the National Communications System, Washington, DC. That support is gratefully acknowledged.

Certain commercial systems, equipment, and telecommunications services are identified in this report so as to adequately develop the concepts presented, explain the functions that comprise network management, and describe typical products that are available to perform network management functions. In no case does such identification imply any recommendation or endorsement by the National Telecommunications and Information Administration. Neither does this identification imply that any of these systems, equipment, or services are the best available for the purpose.

There also are product and service names, such as DOS, UNIX, and Centrex, used in this report that have trademark or registered trademark status. However, that status is not acknowledged in the customary manner, e.g., UNIX™ or Centrex®. There is no intention by the National Telecommunications and Information Administration or the U.S. Department of Commerce, either intended or implied, by these omissions to ignore or infringe upon the recognized trademark ownerships. Rather, the appropriate acknowledgments have been omitted because we find such practice is widespread in the technical literature, and we are unable to be consistent and thorough in determining and using the appropriate acknowledgments.

This report describes the development of network management standards, as well as the organizations involved, and the characteristics of typical commercial products for network management as these components of the technology existed and were available in 1992.

CONTENTS

CONTENTS (cont.)

FIGURES

Page

FIGURES (cont.)

Page

TABLES

Page

ACRONYMS AND ABBREVIATIONS

ACD	Automatic Call Distribution
ACSE	Association Control Service Element
ACTS	Advanced Communications Technology Satellite
ADP	Automatic Data Processing
AG	Advisory Group
AI	Artificial Intelligence
ANSC	American National Standards Committee
ANSI	American National Standards Institute
AO&M	Administration, Operations, and Maintenance
AOM&P	Administration, Operations, Maintenance, and Provisioning
AOW	Asian - Oceania Workshop
ARCAN	ARCnet Analyzer (Anasys, Inc. product)
ASE	Accredited Standards Committee
ASC T1	Accredited Standards Committee for Telecommunications
ASC X3	Accredited Standards Committee for Information Processing Systems
AT&T	American Telephone and Telegraph Company
ATM	Asynchronous Transfer Mode
B-ISDN	Broadband Integrated Services Digital Network
BER	Basic Encoding Rules
BH	Busy Hour
BOC	Bell Operating Company
CBEMA	Computer and Business Equipment Manufacturers Association
CBIS	Cincinnati Bell Information Systems
CCIR	International Radio Consultative Committee
CCITT	International Telegraph and Telephone Consultative Committee
CCS	Common Channel Signaling
CD	Committee Draft
CDR	Call Detail Recording
CEPT	European Conference of Posts and Telecommunications
CME	Conformant Management Entity
CMIP	Common Management Information Protocol
CMIS	Common Management Information Services
CMISE	Common Management Information Services Element
CMOL	CMIP Over Logic Link Control (LLC)
CMOT	CMIP Over TCP
CNOM	Committee on Network Operations and Management
CO	Central Office
COS	Corporation for Open Systems
CPE	Customers Premises Equipment

ACRONYMS AND ABBREVIATIONS (cont.)

CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CSU	Channel Service Unit
CTR	Conformance Test Report
DCN	Data Communications Network
DEC	Digital Equipment Corporation
DIP	Dual In-line Package
DIS	Draft International Standard
DISA	Defense Information Systems Agency
DoC	Department of Commerce
DoD	Department of Defense
DoE	Department of Energy
DoS	Department of State
DOS	Disk Operating System
DoT	Department of Transportation
DP	Draft Proposal
DPN	Data Packet Network (prefix for Northern Telecom products)
DSU	Data or Digital Service Unit
EC	European Community
ECMA	European Computers Manufacturing Association
ECSA	Exchange Carriers Standards Association
EIA	Electronic Industries Association
EMA	Enterprise Management Architecture
EMUG	European Manufacturers User's Group
ENM	Enterprise Network Management
EPRI	Electrical Power Research Institute
ESP	Enhanced Service Provider
ETSI	European Telecommunications Standards Institute
FAX	Facsimile
FCC	Federal Communications Commission
FDDI	Fiber Digital Data Interface
FIPS	Federal Information Processing Standards
FTAM	File Transfer, Access and Management
FTS	Federal Telephone System
FTSC	Federal Telecommunications Standards Committee
GC	Global Control
GNMP	Government Network Management Protocol
GOSIP	Government Open System Interconnection Profile
GSA	General Services Administration

ACRONYMS AND ABBREVIATIONS (cont.)

HDMS	High Density Management System (Microcom, Inc. product)
HP	Hewlett-Packard Company
I/O	Input/Output
IA	Implementation Agreement
IAB	Internet Activities Board
IBM	International Business Machines
ID	Identification
IEC	International Electrotechnical Commission (or)
IEC	Inter-Exchange Carrier
IEEE	Institute of Electrical and Electronic Engineers
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IFIP	International Federation for Information Processing
IILC	Information Industry Liaison Committee
INM	International Network Management
INMS	Integrated Network Management Service (offered by MCI)
IP	Internet Protocol
IRTF	Internet Research Task Force
IS	International Standard
ISDN	Integrated Services Digital Network
ISG	(related to NYNEX)
ISO	International Organization for Standardization
ISP	International Standardized Profile
ITU	International Telecommunications Union
IWS	Integrated Work Stations
JTC 1	Joint Technical Committee 1
LAN	Local Area Network
LC	Local Control
LCN	Local Communication Network
LEC	Local-Exchange Carrier
LLC	Link Level Control
LM	Layer Modules
LPP	Lightweight Presentation Protocol
MAN	Metropolitan Area Network
MAP	Manufacturing Automation Protocol
MCI	Microwave Communications, Incorporated
MD	Mediation Device

ACRONYMS AND ABBREVIATIONS (cont.)

ME	Managed Element
MEM	Managed Element Management
MHS	Message Handling System
MIB	Management Information Base
MIS	Management-Information System
MIT	Management Information Tree
MN	Management Network
MS	Management Solution
MSI	Management Services Interface
MTS	Mobile Telecommunication System
MUX	Multiplex or Multiplexer
NAMS	Network Analysis and Management System (Digilog, Inc. product)
NCMS	Network Control and Management System (NEC America, Inc. product)
NCSL	National Computer Systems Laboratory
NE	Network Element
NICE	Network Information Control Exchange (DEC, Inc. product)
NIST	National Institute of Standards and Technology
NIU	North American ISDN Users (Forum)
NM	Network Management
NMA	Network Management Architecture
NMC	Network Management Center
NMCS	Network Management Control System (Tellabs, Inc. product)
NMF	Network Management Forum
NMS	Network Management System
NMSC	Network Management Subcommittee
NMSIG	Network Management Special Interest Group
NMVT	Network Management Vector Transport
NOS	Network Operating System
NREN	National Research and Education Network
NTIA	National Telecommunications and Information Administration
NTM	Network Traffic Management (AT&T term for Network Management)
OAM&P	Operations, Administration, Maintenance and Provisioning
OICS	Object Implementation Conformance Statements
OIW	OSI Implementors Workshop
OIM	OSI Internet Management
ONA	Open Network Architecture
OS	Operations System
OSI	Open Systems Interconnection
PABX	Private Automatic Branch Exchange
PAD	Packet Assembler/Disassembler

ACRONYMS AND ABBREVIATIONS (cont.)

PBX	Private Branch Exchange
PC	Personal Computer
PCS	Personal Communication System
PDN	Public Data Network
PICS	Protocol Implementation Conformance Statements
POP	Point of Presence
POSI	Promoting Conference for OSI (Japan)
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephone Network
PTT	Postal Telephone and Telegraph
RFC	Request for Comment
ROSE	Remote Operations Service Element
SDH	Synchronous Digital Hierarchy
SEC	Secretariat
SICS	SMASE Implementation Conformance Statements
SIG	Special Interest Group
SMAE	System Management Applications Entity
SMASE	Systems Management Service Element
SMDR	Station Message Detail Recording
SMDS	Switched Multi-megabit Data Service
SMI	Structure of Management Information
SNA	Systems Network Architecture
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SPAG	Standards Promotion and Applications Group
T1	Digital transmission service at 1.544 Mbps that provides 24 voice circuits using two wire-pairs (or
T1	Accredited Standards Committee for Telecommunications
T1M1	Technical Committee for Internetwork Operations, Administration, Maintenance and Provisioning
TAG	Technical Advisory Group
TC	Telecommunications
TCP/IP	Transport Control Protocol/Internet Protocol
TIA	Telecommunications Industry Association
TMN	Telecommunications Management Network
TMS	Telephone Management System
TOP	Technical Office Protocol

ACRONYMS AND ABBREVIATIONS (cont.)

UAOS	User Alliance for Open Systems
UDP	User Datagram Protocol
UNMA	Unified Network Management Architecture
UPT	Universal Personal Telecommunications
U.S.	United States
VGA	Video Graphics Adapter
VPLN	Virtual Private-Line Network
VTP	Virtual Terminal Protocol
WAN	Wide Area Network
WD	Working Draft
WG	Working Group
WS	Workstation
X3	Accredited Standards Committee Information Processing Systems

NETWORK MANAGEMENT:
A REVIEW OF EMERGING CONCEPTS, STANDARDS, AND PRODUCTS

R.D. Jennings, R.F. Linfield, and M.D. Meister*

The objectives of this report are (1) to identify and examine various divergent perspectives that exist about the technology termed network management; (2) to develop a conceptual definition and understanding of network management that is rational and comprehensive; and (3) to examine the questions of what is involved in supporting and controlling a network, what is being done or needs to be done to provide that support and control, and who is involved in doing it. Consistent with these objectives, the report presents a conceptual explanation of network management that is admittedly idealistic, describes the many organizations that are actively involved with the development of real-world, network management standards, examines the functional characteristics of a variety of network management products (available in 1991/92), and discusses some of the important issues and trends that are creating new requirements for network management.

Key words: network management, network management systems, standards

1. INTRODUCTION

The topic of this report is network management (NM)—what it is today, how it is evolving, who is working on it, and how it may change in the future. Many have asked, "What is network management?" and many answers have been given.

For example, a definition given by Freeman (1989), in discussion of data networks and their operation, is the following:

> "Network management means somewhat different things to different people. One can argue that the term is synonymous with technical control. For this discussion, consider the terms the same.
>
> Many conjure up a view of technical control, a military communications term, as banks of patch panels where all circuits of interest can be bridged or terminated for testing. They also can be rerouted in case of poor performance or failure. Network management also includes the traffic flow function and its control, although this function is automated in some of the higher-level protocols and in

* The authors are with the Institute for Telecommunication Sciences, National Telecommunications and Information Administration, U.S: Department of Commerce, Boulder, CO 80303-3328.

International Telegraph and Telephone Consultative Committee (CCITT) Signaling System No.7."

Terplan (1989), at a network management and control workshop[1] that primarily was concerned with networks to connect (and inter-connect) terminals and computers, gave the following definition for network management:

> "Network management means deploying and coordinating resources in order to plan, operate, administer, analyse, evaluate, design and expand communication networks to meet service level objectives at all times, at a reasonable cost, and with optimum capacity."

In the book entitled *Engineering and Operations in the Bell System* (Rey, 1983), network management is described as the function that keeps the network operating near maximum efficiency when unusual traffic patterns or equipment failures would otherwise cause network congestion and inefficiency. The Bellcore *Network Management Handbook* (1989) presents a very similar definition of network management:

> "Network management is the term used to describe a variety of activities associated with improving network traffic flow and customer service when abnormal conditions (unusual traffic patterns or equipment failures) ultimately may have resulted in a congested, inefficient network."

To provide perspective for the Bellcore definition of network management, we note that the Bell system book (Rey, 1983) devotes four chapters to telephone company operations, describing operations as being divided into three kinds of functions—provisioning, administration, and maintenance.

> "**Provisioning** is the process of making the various telecommunications resources (such as switching systems, transmission facilities, and operators) available for telecommunication services. Provisioning includes forecasting the demand for service, determining the additions (or changes) to the network that will be needed, determining where and when they will be needed, and installing them.
>
> **Administration** covers a broad group of functions that sustain services once they have been provided. Administration generally consists of **network administration** and **service administration**. Network administration ensures that

[1] The Network Management and Control Workshop, held September 19-21, 1989, in Tarrytown, NY, and jointly sponsored by the (New York) Polytechnic University, the New York State Science and Technology Foundation and its Center for Advanced Technology in Telecommunications (CATT), NYNEX Corporation, and the IEEE Communications Society's Committee on Network Operations and Management (CNOM).

> the network is used efficiently and that grade-of-service objectives are met. Service administration includes such diverse functions as billing; collecting and counting coins from coin telephones; and, for customer switching system, giving engineering and service evaluation assistance and keeping detailed engineering records.
>
> **Maintenance** operations ensure that network components work properly once they are installed. Maintenance includes the testing and repair activities that correct existing malfunctions (corrective maintenance) and those that prevent service-affecting malfunctions (preventive maintenance)."

A recent technical paper on the evolution of network management at the American Telephone and Telegraph (AT&T) Company (Wetmore, 1991) makes the following observation:

> "The practice of network management has undergone significant changes at AT&T over the last five years. ...the definition of the term "network management" has changed as well. **Today, this term is used to apply to many of the functions related to the operation, maintenance and administration of a telecommunication network.** (Emphasis added) That is why AT&T has begun using a more specific term—network traffic management (NTM)—to refer to the discipline formerly known as network management."

Wetmore's paper primarily discusses the changes that AT&T has implemented in developing their current practices of *network traffic management.*

Material that describes military telecommunication systems often uses the words (and acronyms) Administration, Operations, and Maintenance (AO&M) or Administration, Operations, Maintenance, and Provisioning (AOM&P) in discussing the telephone company operations functions defined above. These functions often, but not always, include the functions of network management.

Other views of network management, that often are similar to the definitions given above, have been expressed in the literature. (See, for example, Caruso, 1990; Flanagan, 1990; Herman, 1989; and Valovic, 1987.) The management associated with local area networks (LANs) is the basis for one of the most common and widespread interpretations of network management.

Organizations that have been and are developing standards for network management (see Section 3) also have defined network management. For example, management for Open Systems Interconnection (OSI) networks is defined by the International Organization for Standardization (ISO) in conjunction with the International Electrotechnical Commission (ISO/IEC) (1989) as:

> "The facilities to control, coordinate and monitor the resources which allow communications to take place in the OSI Environment."

There is no single, clear definition for network management given by the International Telegraph and Telephone Consultative Committee. For example, Recommendation X.200 (CCITT, 1989e) that defines the reference model of open systems interconnection for CCITT applications contains no explicit definition for network management. However, this Recommendation is closely aligned with the ISO 7498 Standard (1984) that defines the basic reference model for open systems interconnection for information processing systems. It seems reasonable, therefore, to conclude that a definition very similar to the ISO/IEC definition cited above for network management would apply.

Recommendation E.410 (CCITT, 1989b) presents general information concerning international network management and defines network management as:

> "... the function of supervising the ... network and taking action when necessary to control the flow of traffic."

Note the emphasis on traffic control in this definition.

Another view of network management is suggested in Recommendation M.30 (CCITT, 1989d) which presents principles for a Telecommunications Management Network (TMN) for international transmission systems and telephone circuits. Again, no explicit definition is given for network management, but text of the Recommendation indicates that the TMN provides an organized structure to achieve network management, and that management includes performance management, fault (or maintenance) management, configuration management, accounting management, and security management. These are the functions necessary to cover operations, administration, maintenance, and provisioning of a telecommunication network.

Finally, the CCITT definition given for network management in Volume I (CCITT, 1989a) that contains terms, definitions, abbreviations, and acronyms is:

> "The activity performed ... to regulate traffic flow."

This definition is referenced to and exactly the same as that given in Recommendation Z.337 (CCITT, 1989f) that is concerned with network management administration.

The definition that we offer that is broad and general and that will be followed in this report, unless explained otherwise, is developed from basic definitions for ***network*** and

management. This definition applies to all types of telecommunication networks and the services that these networks provide.

The Institute of Electrical and Electronics Engineers (IEEE) Standard Dictionary of Electrical and Electronics Terms (Jay, 1988) does not define network management, but it contains several definitions for ***network***. Pertaining to communications, particularly data transmission, ***network*** is defined as

> "A series of points interconnected by communication channels."

Pertaining to software, ***network*** is defined as

> "An interconnected or interrelated group of nodes."

Webster's Dictionary (Gove, 1976) defines ***network*** (in part) as

> "**2:** a system of lines or channels that interlace or cross like the fabric of a net **4:** a system of electrical conductors in which conduction takes place between certain points by more than one path."

Federal Standard 1037B (GSA, 1991) defines ***network*** as

> "**1.** An interconnection of three or more communicating entities and (usually) one or more nodes. **2.** A combination of passive or active electronic components that serves a given purpose."

In fact, there are many types of networks. These networks usually are classified by applying criteria, either independently or in combination, such as the service(s) offered, the geographic area(s) covered, the customers served, and the way in which the network is implemented.[2] In this report, a generic meaning for "the network" is intended unless a more specific definition is needed or clearly implied by the context of the discussion. From all of the definitions cited above, the generic definition for ***network*** that we use is

> An interconnected group of communicating entities and nodes (e.g., telephones, terminals, computers, circuits, and switches).

[2] Networks classified by the offered services may be grouped as voice networks, data networks, imagery networks, etc. Those classified by the area(s) to which services are provided include local, national, enterprise-wide, and global networks. Networks classified by the way in which the network has been implemented include, for example, circuit-switched, packet-switched, and message-switched networks. Networks often are classified as public or private networks, and whether the network is used for interconnecting computers, terminal operators, businesses, or other entities.

Before proceeding further with the definition of network management, some additional comments about the term "network" (or networks) are appropriate. The term is used frequently in this report with a rather broad range of meanings. Several formal definitions for network have been given, along with the generic definition that we prefer and use. The formal definitions of two closely related terms, taken from proposed Federal Standard 1037B (GSA, 1991) also are important to note:

> **network architecture** — 1. The design principles, physical configuration, functional organization, operational procedures, and data formats used as the basis for the design, construction, modification, and operation of a communication network. 2. The structure of an existing communication network including the facilities, operational structure and procedures, and the data formats.
>
> **network topology** — The specific physical (real) or logical (virtual) arrangement of the elements of a network. Note: Two networks have the same topology if the connecting configuration is the same, although the networks may differ in physical interconnections, distance between nodes, transmission rates, and signal types.

These terms and other related terms are discussed in a report on telecommunication networks, services, architectures, and implementations by Linfield (1990).

Consistent with these definitions, the term "network" is used in many ways to describe networks from either the providers' or the users', or sometimes both, viewpoints. Some of the most common types of networks are identified below.

- The public switched telephone network or PSTN.
- The public data network or PDN.
- An integrated services digital network (ISDN), that may be either public or private, and that may include a local area network or wide area network. Such networks, today, exist only as "islands" of integrated services.
- (The networks identified above may be considered from either the providers' or users' viewpoints. The networks identified below most commonly are considered from the users' viewpoint.)
- A user's network that uses either the PSTN or the PDN and may include a local area network or wide area network.

- A user's private network that may include a local area network or wide area network.

- A user's private network that uses either the PSTN or the PDN. Such networks may include a local area network or wide area network.

Many other types of networks may be imagined that would use mixtures of components and involve either the public switched network, a private network, or both. An example would be a virtual private network (VPN), a service that is offered by an interexchange carrier (IEC) to provide customers the benefits of a premises-to-premises voice and data private tandem network without requiring private tie trunks across the network. A VPN exists as a private network embedded in the IEC's switched public network. The VPN is software defined and only appears to have dedicated switching and transmission facilities. These facilities, in fact, are physically shared with other public network users.

Our discussion of the network sometimes may represent the perspective of the provider and at other times the perspective of the user. Users' networks often are heterogeneous because of the several network architectures[3] that usually are involved. An example of a user's network that uses today's PSTN is illustrated in Figure 1. This network shows CPE at one node with a PABX connected through the PSTN to CPE utilizing Centrex services at the other node. The CPE at each of these network nodes includes a variety of terminal equipment such as telephones, personal workstations (WSs), facsimile equipment, and host computer systems serving remote terminals, as well as local area networks that can include additional, similar terminal equipment. We observe that such a network can include many separate network management capabilities. In principle, the user's network also may include satellite links as normal transmission capabilities or as back-up transmission capability for the terrestrial transmission network. In the near future, these satellite links may be provided by satellites, such as the Advanced Communications Technology Satellite (ACTS), that have on-board switching and narrow, directive antenna beam capabilities.

[3] Various meanings of the general term network architecture are defined and discussed by Linfield (1990). Very briefly, one important distinction is that network architecture may be understood to be the physical arrangement and connectivity of the network elements, and this often is described as the physical network architecture. Another common understanding, however, of network architecture concerns the protocols that are used for communication, and this often is described as the functional network architecture.

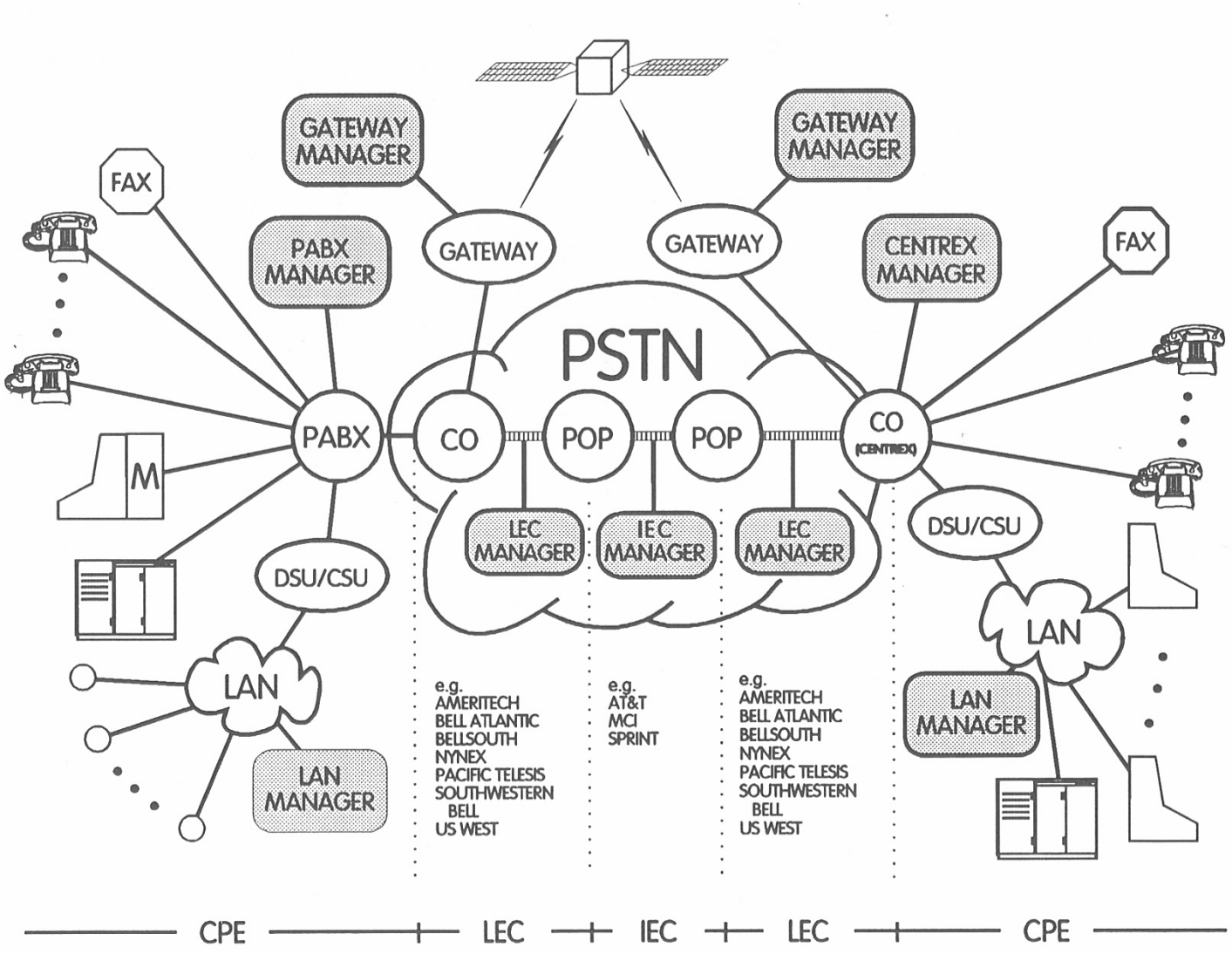


Figure 1. Illustration of a possible user's network that uses today's Public Switched Telephone Network.

A somewhat more abstract illustration (compared to Figure 1) of a possible user's network with an ISDN type of node added is shown in Figure 2. The "switched network" part of this illustration is composed of multiple switched networks that include local-exchange carriers (LECs) and IECs providing circuit-switched networks, packet-switched networks (for data), and the common-channel signaling network that also is packet-switched. This figure illustrates types, rather than representative numbers, of nodes and terminal equipment comprising the user's network. The heterogeneity of the network is illustrated by different functionality being defined for each node. Communication between the different functional architectures requires carrier-signal-type and protocol conversions. These conversions are provided by capabilities such as modems, data/channel service units (often referred to as DSU/CSUs[4]), special gateways, etc. or by other capabilities incorporated into the network nodes. Network management in this conceptual, user network would be integrated, distributed, and ubiquitous.

A possible, futuristic and more advanced concept for users' networks is shown in Figure 3, where several important ideas are illustrated. For example, the networks available to users at any given time would contain a spectrum of capabilities, ranging from Plain Old Telephone Service (POTS) to ISDN and, eventually, to broadband-ISDN (B-ISDN) and personal communication systems (PCSs) and Mobile Telephone Service (MTS). Such networks could include LANs, MANs, and WANs that provide integrated services using ordinary telephones and workstations as well as integrated workstations[5] (IWSs) at the users' locations, or customers' premises. Capabilities for B-ISDN and PCS are only in developmental stages, but some IWSs exist today. Similar to the conceptual network illustrated in Figure 2, network management in such an advanced network is expected to be highly integrated, distributed, and completely ubiquitous.

As for the management part of network management, Webster's Dictionary (Gove, 1976) defines ***management*** (in part) as

---

[4] Strictly speaking, a CSU (channel service unit) is a hardware interface between a user's data terminal equipment and a digital link with a central office. The CSU provides line isolation, to protect the network from malfunctions in a user's equipment, and loopback capabilities for network testing. A DSU (data service unit) is a hardware device that provides digital interface between a digital line and an item of data terminal equipment. The DSU provides timing recovery, bipolar conversion, signal generation control, signal recognition, and synchronous sampling. Generally, the DSU includes the CSU functions, the devices often are referred to as DSU/CSU.

[5] Workstations that provide integrated services.

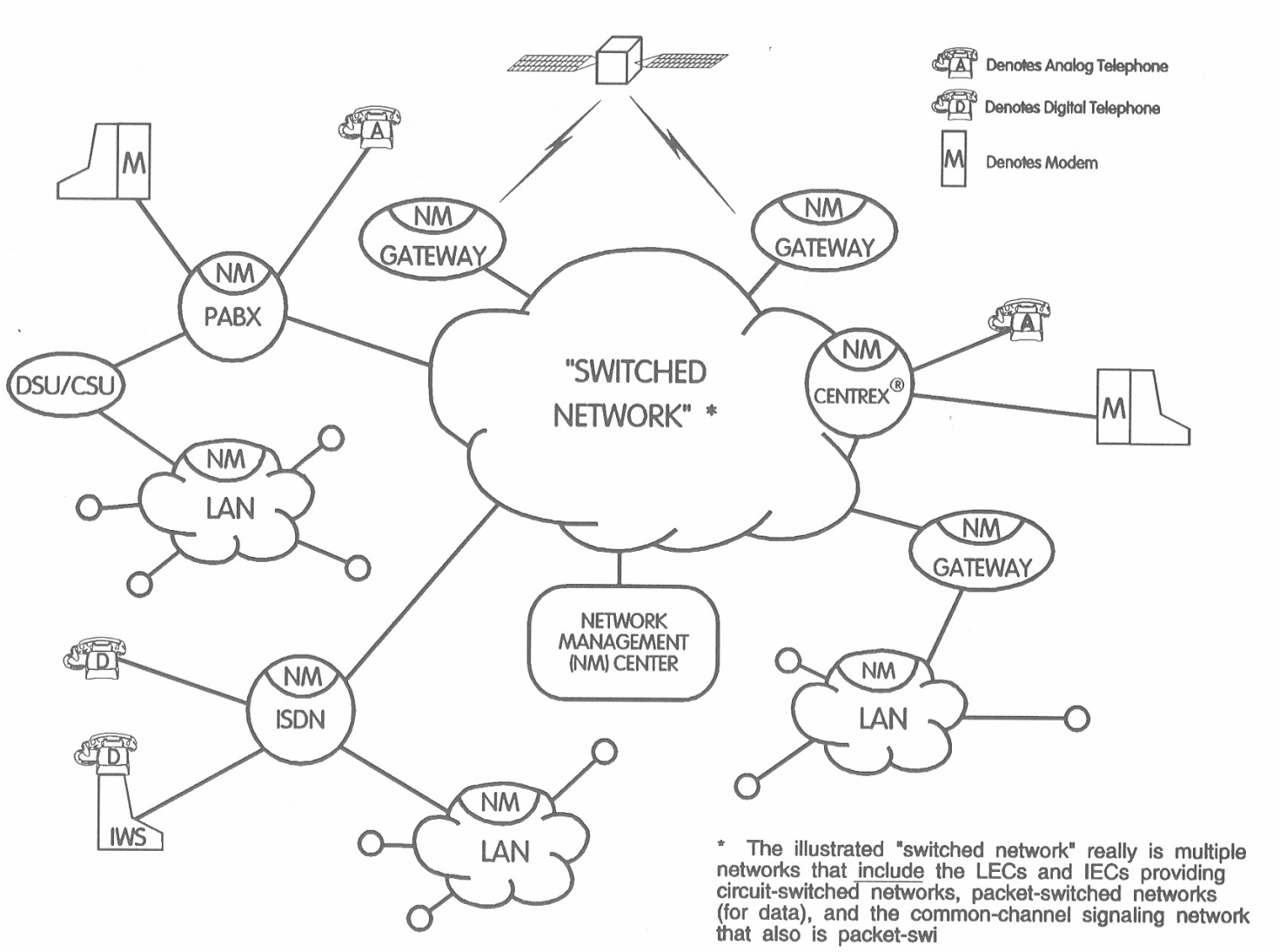


Figure 2. Illustration of another, possible user's network; expanded functionality with the ISDN node and more abstract when compared with Figure 1.

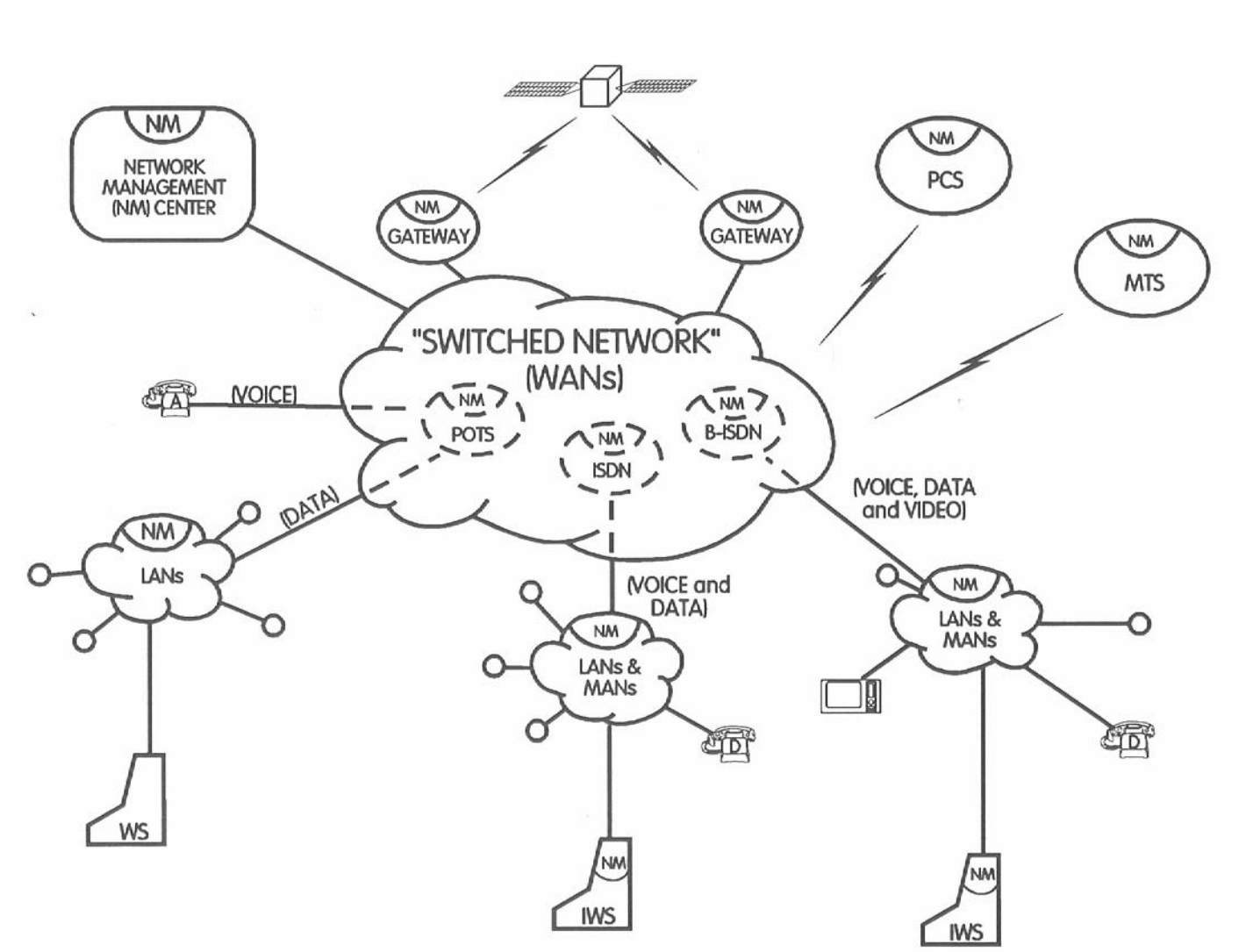


Figure 3. An example of a possible, futuristic and more advanced configuration for a user's network (than illustrated in Figure 2).

> "The act or art of managing as **a:** more or less skilled handling of something **c:** the conducting or supervising of something (as a business); especially, the executive function of planning, organizing, coordinating, directing, controlling, and supervising any industrial or business project or activity with responsibility for results."

From these various definitions for ***network*** and ***management***, we have formulated the following general definition for ***network management:***

> **The act or art, more or less skilled, of supporting and controlling an interconnected group of communicating entities and nodes (e.g., telephones, terminals, computers, circuits, and switches)[6]**

It should be recognized that the skill used in providing support to and control of the network management process may be direct human participation or it may be "skill" built into software and hardware that applies automation and even artificial intelligence (AI).

The threefold objective in this report, then, is

a) to sort through some of the divergent perspectives that exist (and that seem to cause confusion and misunderstanding) about network management

b) to develop a conceptional understanding of network management that is rational and comprehensive and that, intentionally, is not oriented exclusively to data networks or voice networks

c) to examine the questions of what is involved in supporting and controlling a network, what is being (or needs to be) done to provide that support and control, and who is involved in doing it.

Consistent with this objective, the report presents a conceptual explanation of network management in Section 2 that is recognized as idealistic in some cases. In addition to discussing the purpose and scope of network management, functions that are suitable for management are identified. Contrasting perspectives and factors that affect the development and implementation of network management and integrated network management systems are included.

In Section 3 the report discusses the various organizations that are actively involved with the development of network management standards. Typical products, i.e., the systems, that are

[6] In the discussion of network management fundamentals (Section 2), various statements are made concerning network management as it has been understood by others or as it may be understood in a particular situation. These statements are not intended as alternate definitions of network management. Rather, all of these statements should be understood to be covered by, and be a part of, this general definition for network management.

available to assist users and providers with network management are discussed in Section 4. The emphasis is on functional capabilities and capability differences in these products.

Section 5 summarizes the highlights of the report and identifies some issues and trends that are likely to influence the continuing development of network management. Advanced optical fiber technology, broadband integrated services digital networks, expert systems that incorporate artificial intelligence, the introduction and growth of personal communication systems, the diversity of standards, and government regulations are among the topics noted. The conclusions and recommendations that have emerged in conducting this study are collected in Section 6. References cited in the report are given in Section 7.

Three appendices supplement the material presented in the report. Appendix A contains an extensive identification of organizations that are involved with the development of network management standards, showing the inter-relationships between these organizations. Appendix B is a summary description of the OSI Reference Model, and Appendix C is a list of the OSI Network Management Standards.

2. FUNDAMENTALS OF NETWORK MANAGEMENT

For many years, network operations were quite focused. A user simply would specify his service needs to "the telephone company" and that company took the responsibility to plan, design, build, and maintain the necessary capabilities to satisfy those needs. The telephone company would follow its well-defined operations procedures for providing, administering, and maintaining the network and the telecommunications services it provided (briefly described in Section 1). These user-specified, telephone-company-managed, networks were relatively straightforward variations of networks to provide voice telephone service. Most users simply relied on "the telephone company" to take care of all of their service needs, fix their problems, provide the necessary expansions, install the upgrades, and insure quality.

In the 1960s and 1970s, data communications were introduced and information-processing networks, with varying requirements for network quality and capacity to support a variety of new voice-bandwidth services, began to evolve. As the technology matured, more user-controlled devices were connected to the network, and information-processing networking began to change from batch to real-time applications. Divestiture of the Bell System (the AT&T Divestiture Plan

approved August 5, 1983 and effective January 1, 1984) substantially accelerated this trend. The old approach of relying on "the telephone company" to satisfy all networking requirements no longer was a viable option. "The telephone company" simply was not allowed to respond to every user request as before. In addition, the concept and benefits of dynamic network reconfiguration and control (some of the capability provided by network management) began to be realized, thus the need for user-controlled network management was becoming recognized. Though recognized as needed, network management systems that provide extensive user-control are still in the future.

The practices of network management, however, tended to be separated into one set of "standard practices" and capabilities, often utilized by users, for managing the data or information-processing networks and another set of "standard practices" and capabilities, administered by the local and inter-exchange carriers, for managing the voice (telephone) networks. Network management for data communications tended to place emphasis on monitoring and control so as to achieve high quality performance of the network. Network management for telephone networks, on the other hand, tended to place emphasis on administration of the network—"either it worked or it didn't."

Several years ago, Gawdun (1987) reported that market research conducted by Bellcore had identified several functions that could give users additional management and control capabilities (sometimes provided by the carrier) over their network configuration and bandwidth. These included

- time-variant circuit connections
- time-variant bandwidth/bit rates
- real-time disaster recovery
- real-time performance information
- network status information
- reservation capabilities
- time-variant service options.

New technology and other user/business requirements are causing computing and information-processing capabilities to be transformed into distributed environments with requirements for sophisticated interconnecting networks; sometimes referred to as data networks

or information-processing networks. This trend coupled with new technology and users' requests for new services provided by the network are causing Plain Old Telephone Service to be transformed into sophisticated telecommunication networks with considerable processing power[7]. Some examples of the services provided by these sophisticated networks include

- The Public Telephone Network "800" toll-free calling services that are supported by intelligent databases (and sometimes integrated with service to identify the calling party's telephone number—Automatic Number Identification or ANI)

- Virtual private network (VPN) service (an example of AT&T's Software Defined Network service) that provides customers with premises-to-premises integrated voice/data private tandem network service without the need for private tie trunks across the public inter-exchange network (IEC)

- Switched Digital Services to provide short-term, high-data-rate, digital connectivity, such as the Switched Multi-megabit Data Service (SMDS) offered by carriers

- A variety of Messaging Services such as facsimile, paging, and voice and electronic mail

- Common Channel Signaling (CCS) that allows faster and more complex signaling between different parts of the network to remotely control the switching and to support various other sophisticated, intelligent network services.

The distinction between telephone networks and data or information-processing networks is becoming more and more blurred. That trend is continuing as digital transmission services such as T1[8] and fractional T1 become widely available. The introduction of integrated services digital networks, and the planning for future broadband-ISDN, provide integrated access to voice, data, and video services and will further encourage and shape this transition. The "marriage" of telephone and information-processing networks to support this integration has led to the definition

[7] The processing power spoken of here is within the network to support the transport function and intelligent services provided by the network. It is not the distributed computing and information-processing capabilities supported by network interconnections.

[8] In the strictest sense, transmission that used copper-based digital facilities to provide 24 simultaneous voice or data circuits at 64 kbps for each circuit (1.544 Mbps) was introduced as T1 (or T-carrier) service. Today, many T-carrier services are based on fiber optic transmission facilities, rather than copper. However, the term continues to be used and now is understood to refer to any digital carrier service.

of information networks[9] as enablers of the Information Age (Caruso, 1990). Networks to provide these services often include a wide assortment of equipment from a variety of vendors that may use different protocols and interfaces. Many of these diverse equipments often include some "management" capability or system, but only for that particular component.

In this environment, network management is one of the most important, but confusing and least understood, aspects of telecommunication networks. In summarizing users' needs, Caruso suggests that the highest-priority attributes of new network management systems are interoperability of products from different vendors and integration of the capabilities to manage a wide variety of individual network components into a single system-one interpretation of integrated network management. Caruso also notes that the Information Age offers many opportunities and challenges, but that perhaps the greatest challenge is that of managing the telecommunication network resources and services, a challenge that is real to the public carriers as well as each user[10] that has unique, user-defined networks. This is the challenge that has created the relatively new and evolving discipline called **network management**[11].

Day-to-day activities of many organizations are increasingly dependent upon a diversity of telecommunication services. Executives, for example, are discovering that creative use of telecommunication services is key to enhanced revenues and increased profits for their businesses. These usage and economic-importance trends, along with the growing complexity and sophistication of the network, all contribute to the strategic importance of network management.

---

[9] Throughout this report, we use the terms "telecommunication" and "telecommunication networks" rather than "information" and "information networks", as suggested by Caruso (1990), in referring to or describing networks that provide both telephone and information-processing services. Such use is consistent with the definitions of "telecommunication" that are published by CCITT (1989a) and in FED STD-1037B (GSA, 1991).

[10] A "user" is a person, a human operator of a computer terminal, or a computer-application program that processes communicated information (see ANSI, 1983) that is connected to and uses the services provided by a telecommunication network. From a telecommunication network point of view, an "enterprise" is an organization or corporation where many "users" share services that are specified according to the enterprise's objectives and priorities and that are provided by the "enterprise's network".

[11] Some writers use the term, network management, in describing only those aspects of network management that pertain to the lower levels (i.e., the physical, data link, network, and, possibly, transport layers) of the OSI Reference Model (ISO, 1984). The term, integrated network management, often is used to describe network management performed with multi-vendor equipment or to describe the management of networks that provide integrated services. The conceptual definition of network management developed and presented in this report includes all of these aspects of management and, therefore, obviates any need for the term, integrated network management, except in discussion of products for performing network management.

Network characteristics such as high aggregate bandwidth channels with accompanying increased vulnerability to operational failures, increasingly heterogeneous mixes of network components—hybrid networks, etc., are examples of the growing complexity and sophistication of networks. These are the types of factors that are leading users to express their most urgent needs as being network management systems that will allow the interoperability of products from different vendors and the integration of diverse management capabilities.

Managing the telecommunication network resources is considered to be one of the greatest challenges that users and providers of these resources must face. Network management from the end-user's perspective may involve individual control in the use of available telecommunication services. For voice services, available features may include call forwarding, speed calling, multi-party calling, etc. Similar, but often more complex, features for data-communication services also may be available. Such features might include ability to update user profiles and provide real-time, interactive information to the network in order to define and control required data communication services.

Often, the end-users' requirements are aggregated and processed by an enterprise's communications manager. This manager's authority might include ability to reconfigure software-defined networks embedded in the Public Switched Telephone Network (PSTN), reconfigure private, leased-line networks, or make station rearrangements for the central rather than private switching services (e.g., Centrex[12] in lieu of a private branch exchange (PBX) or private automatic branch exchange (PABX)). Other responsibilities could include planning, ordering and installing, configuring, repairing, accounting and billing, reporting, and controlling network security.

The increasing complexity and sophistication of networks, the rising percentage of total business costs that derive from telecommunication services, as well as opportunities to reduce costs (for a provider) or expenses (for a user) and save dollars, all underscore the growing importance of network management. Many factors contribute to the complexity of network management from both the service-users' and the service-providers' perspectives; such factors

[12] Centrex is a switching service provided by physical and logical partitions within the Central office so as to provide calling features normally provided by a PBX. These features may include ISDN, automatic callback, automatic redial, customer-originated trace, calling number delivery blocking, calling number display, voice messaging, station rearrangement, station message detail recording (SMDR), and Automatic Call Distribution (ACD).

include the many commercial information-processing standards and procedures and the multiplicity of networks, e.g., the public telephone network, packet-switched data networks, ISDN, and a variety of private, dedicated networks,

The need for network management is solidly established by the natural growth in size and complexity of networks and the expanding services provided by these networks, as well as the sharply increasing reliance of businesses on telecommunication services for meeting their profit objectives. But, the importance (and burden) of user participation in the management or control of the network also has increased dramatically since divestiture of the Bell System that led to the subsequent division of public telecommunication networks into the following four major domains:

- the inter-exchange (or long-distance) carriers (IECs)
- the intra-exchange (or local-exchange) carriers (LECs)
- the customers' premises, with customer premises equipment (CPE)
- the information service providers (who may include third-party network management service providers).

Summarized, the situation today is—

- increasing numbers of users
- increasing numbers and types of equipment (from many different vendors, with different interfaces and protocols) that users want to connect to their networks
- increasing opportunities to provide the telecommunication connections (networks) between this widely diverse equipment.

2.1 Purpose and Scope of Network Management

Caruso (1990) has noted that the telephone network provides the earliest example of network management, where telephone operators could detect network problems and initiate maintenance and repair efforts. The direct participation of operators in establishing each call dramatically changed in the 1950s, however, with the introduction of direct distance dialing. Then, stored-program-control switches (introduced in the 1960s) and computerized operations systems (introduced in the 1970s), with software- rather than hardware-controlled operation,

provided the capability for sophisticated and centralized network monitoring, data collection, and network control, collectively called network management. This was network management from the perspective of the provider, and customers generally realized very high reliability and availability of the offered services. Then, as network services became more sophisticated, it was recognized that customers' business successes were critically dependent on judicious use of these new features, so services known as customer network management services became available. Some examples are a user's ability to change the call-forwarding number, the speed dialing selections, or to rearrange connectivity (a Centrex service feature).

As a result of the Bell-system breakup and the "digital revolution in network design" (Flanagan, 1990), there are strong, new trends in networking technology. For many years, most users' networks were voice-grade lines that may have carried voice or data (with the use of modems). However, since the introduction of digital carrier systems (in the early 1960s) and the offering of tarriffed digital services (e.g., T1 service in 1983), the separate operational domains for analog and digital services (that include voice service) have also resulted in separate network management systems for each domain. These individual-domain, network management systems and practices provide no single point from which it is certain that all of a user's network connections and services can be managed. There is no "single view" of the end-user's entire network, and, in fact, some portions of that network are completely unmanaged and inaccessible to be managed. In today's growing digital-networks environment, this is regarded as a very undesirable situation.

Noting that a variety of network management issues remain unresolved, Cassel et al., (1989) have identified four general issues that are relevant to all areas of network management. These general issues are:

> **What functionality is needed?** Different communities of interest continue to perceive different network management needs that require different solutions. In other words, what are the essential functions that must be provided in network management?
>
> **How far do we standardize?** Agreement on the functions that must be provided for management of the network does not solve all of the problems. In general, and for a variety of reasons, implementations of the same functionality will be done in different ways by different hardware and software developers. The result is network heterogeneity. Management of the network, however, requires direct access to detailed information about the network and the ability to manipulate

many network characteristics. Thus, the issues arise: What parts of the network must or should be standardized? And, where should the network allow for proprietary characteristics?

How well will the system scale? Much of the current interest in network management follows from the recognition that many "existing networking systems" are growing very rapidly (suggested to be in excess of 100% per year). This growth is challenging network users and providers alike to develop new management systems that will support very large networks (perhaps containing millions of nodes).

How fast can we expect existing networks to change? In general, the more complex and innovative the network management system, the longer it will take to upgrade an existing network to support it. An anticipated deficiency of information required by a more complex or innovative network management system can become the basis for using less complex systems that only address immediate and obvious needs, while less pressing needs may allow the freedom to develop complete systems. Note, however, that this general rule for matching networks and management systems is not hard and fast; complex and powerful management systems have been proposed for networks with immediate needs, and simple systems have been proposed for less developed networks.

Generally stated, the purpose of network management is to help users efficiently and effectively use their diverse telecommunication resources so as to receive maximum service benefits and to help providers use their resources efficiently so as to enhance profitability. More specifically, the purpose of network management, for both users and providers, is to maximize availability and performance of the telecommunication resources within the scope of three basic functional areas suggested by Valovic (1987) as:

Monitoring and control: Observing the performance of the network equipment and making changes, as necessary in the operating parameters. These functions usually involve short-term or real-time adjustments to configuration of the network.

Administration: A wide range of day-to-day tasks such as adding new users to the network, maintaining accurate inventory of the network assets, billing for use of the network, dynamically reconfiguring the network, as required, etc. These functions usually involve medium-term, e.g., hourly or daily, adjustments to configuration of the network.

Planning and design: The on-going process of revising the design of the network, as may be required, and re-optimizing use of the network while giving

consideration to the users' needs. These functions usually involve long-term, e.g., yearly, adjustments to configuration of the network.

One aspect of the scope of network management is that it is a multi-dimensional discipline that combines pre-implementation activities, such as planning, analysis, and design of the network, with many operational activities, that include administration, maintenance, and control. The historical responsibilities for managing the network within each of the domains noted earlier give rise to questions about other aspects of the scope of network management today and into the future. Such questions include: "How much control should an end-user have over a carrier's circuit and switches?"; "How can a user truly realize end-to-end management of his/her network?"; "How far into the customer's premises should a carrier's management capabilities extend?"; or "What options are available for a carrier to cope with disruptions to major sections of his network?"

Most networks will include many switching nodes and terminations. These nodes will contain a diverse mixture of different vendors' equipments (e.g., switching equipment, multiplexers, concentrators, computer terminals, etc.). The nodes are likely to be connected using a variety of transmission media (e.g., open-wire lines, paired and coaxial cables, fiber-optic cable, terrestrial microwave radio, satellite, etc.). The network may include LANs, a wide area network (WAN), a metropolitan area network (MAN), or any combination. Connections through the network could include, or be in addition to, normal connections to a private network or to the local- and inter-exchange carriers of the public network. Because of the diversity of equipment connected to the network and the diverse ways in which telecommunication connections may exist between the nodes, the users' equipment (e.g., host computers, terminals, PABXs, etc.) may be unable to inter-communicate. These mixed equipment need to be able to provide information to and receive instructions from a central computer that understands the "language" of each type of equipment and the topology of the entire network. Flanagan (1990) calls this central computer a "mediator," and suggests that the technology is available for "mediator" functionality that can extend network management capability to the ends of the network.

In effect, the concepts that we have just described explain one aspect of integrated network management[13]. Subsequent subsections examine how this scope for network management might be realized. A conceptual network-management architecture is illustrated in Figure 4. The network would consist of many users and a diverse mixture of different vendors' equipment using today's Public Switched Telephone Network to provide the telecommunication connections between customer premises equipment.

For an integrated network management capability, this architecture shows the network manager's (or users') access to and control of network elements in the customer premises, LEC, and IEC domains. The network management capability is connected directly to vendor-specific network management capabilities for the customer premises domain. It is connected to network management gateways for the local-exchange and inter-exchange carriers' domains. These gateways provide the connections or interfaces to the various vendor-specific network management capabilities and associated network elements in these domains. In addition, connections between vendor-specific network elements in the customer premises' and local-exchange carriers' domains are shown. Standard interfaces and protocols between the various network management systems and between the network management systems and the network elements would provide substantial improvement to interoperability.

The developing technology of advanced communications satellites[14] may offer significant new capabilities for augmentation and/or restoration of telecommunication services that are provided by the public switched telephone network, a network that today is largely made-up of terrestrial elements for switching and trunking. The concept of services provided by a hybrid network composed of both advanced-technology, terrestrial and communications-satellite components is described and discussed by Nesenbergs (1991). This revolutionary composition for a hybrid network, that could be either private or public, will require new interfaces, both

[13] Other aspects of integrated network management have to do with networks that are managed using the OSI/ISO-based methodology for packet-switched networks and the methodology recommended by the CCITT (1989d), namely Telecommunication Management Networks, for circuit-switched networks, as well as the management of networks that provide integrated services, e.g., voice, data, and video services.

[14] In the context of this report, on-board signal processing, rapidly switchable, spot-beam antennas, and the use of carrier frequencies in the 30/20-GHz band are the principle new technologies that are associated with advanced communications satellites. The on-board signal processing and spot-beam antenna technologies are most relevant to the development of a hybrid public switched network.

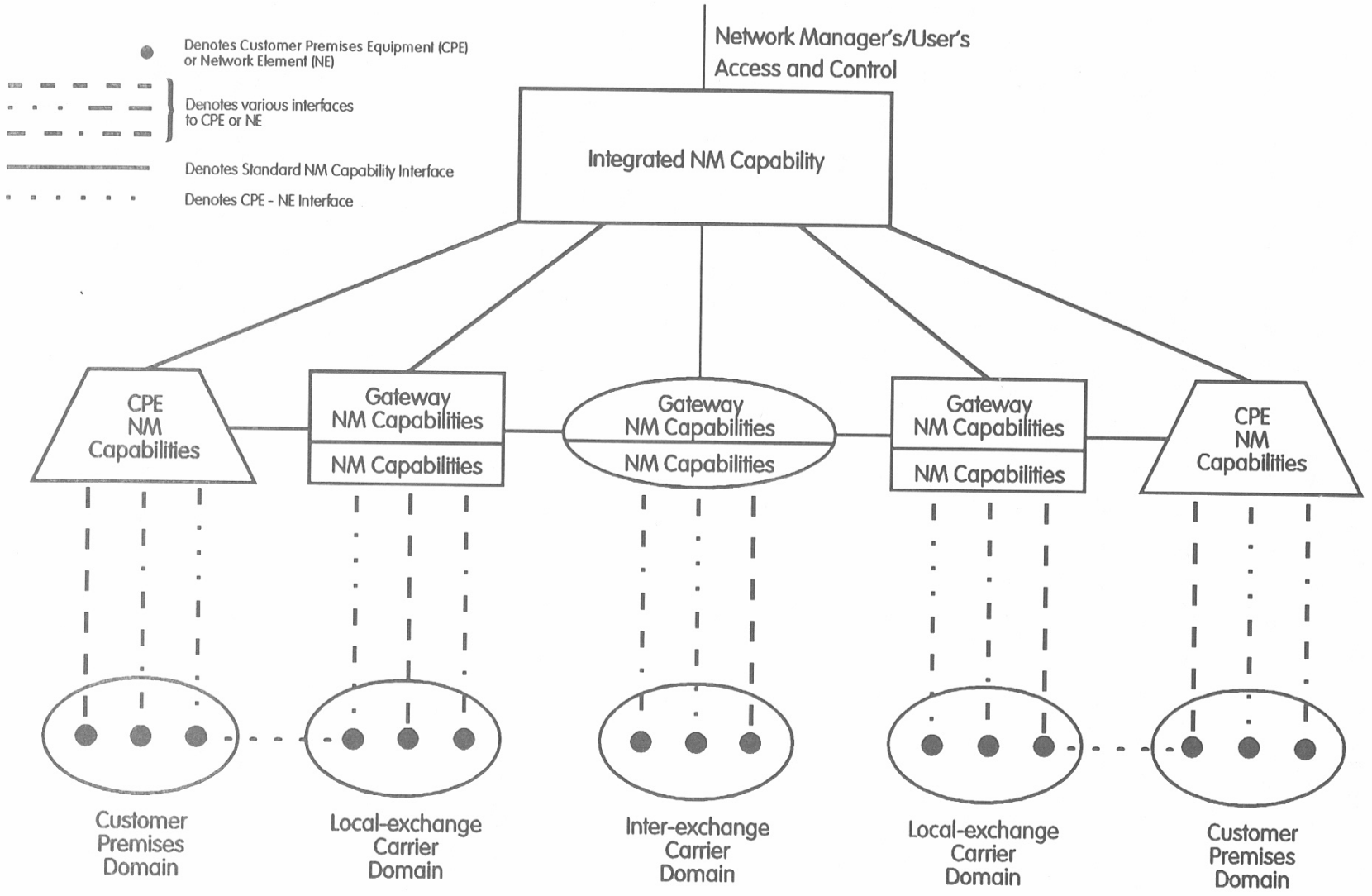


Figure 4. A conceptual network-management architecture (based on Caruso, 1990).

physical and functional, to be defined. New specifications and standards also will be required to define the inter-operation of these hybrid networks. These specifications and standards will need to interact and be aligned with existing network management practices and standards.

2.2 Basic Concepts of Network Management

Many people seem to believe that managing telecommunication resources requires only the right hardware and software; that is, get the "right tools" (Frank, 1988 and Herman, 1989). There may have been a time when that was possible, but the complex, dynamic networks that users demand and are using today cannot be managed adequately by simply connecting a bewildering array of "boxes that blink and buzz" (e.g., many separate, vendor-specific, network management tools) to the network. As Frank and Herman and others suggest, the discipline of network management is a multi-dimensional, continuing process; it is a series of actions, changes, and functions, repeated as often as necessary, that help users realize efficient and effective use of their telecommunication resources.

In this section of the report, we first define and discuss the overall process of network management, before we examine the specific functions that are involved. A complex process often is understood and defined most usefully by applying a systematic approach to the problem. Such an approach has been followed by others, and we use some of their ideas in this discussion (for example, see the papers by Willetts, 1988 and 1991, and Bohm and Ullmann, 1989). The approach is conceptual and based largely upon an application of management techniques rather than on applications of technology that have been (or could be) developed and offered specifically for network management. (Section 4 discusses network management systems and capabilities that are available today.)

The approach considers network management to be a management process that is applicable to all of the telecommunication resources (i.e., the network, the network elements, and the services provided by the network) independent of any specific network architecture. (Various architectures for implementing the network management process are defined and discussed before considering the functions that are suitable for management.) The approach allows us to define and describe a conceptual, network management capability, that is integrated by design, with the hope that such network management capability could replace the collection of discrete but individually-limited capabilities that often are being used today.

Every organization performs essential functions and has support requirements that we assume can be provided by an information processing system that is part of the total assets of the organization. The system may be large or small and provide multiple services or a single service, but just as for the other assets of the organization, it must be planned, designed, installed, used, repaired, modified as needs change, etc.; in other words, it must be managed. The information processing system would consist of hardware, software, and procedural facilities for which Böhm and Ullman (1989) have suggested the conceptual structure shown in Figure 5. The system would be divided into three, layered parts, each with its own management capabilities: (1) the application (sub)system, (2) the distributed, processing-support (sub)system, and (3) the communication (sub)system. The communication (sub)system is considered to be a general capability that provides both telephony and data communications.

The **application (sub)system** would consist of all the applications (pertaining to the information processing system) and the relationships between them that would result in interactions between the applications. These applications would be described in terms specific to the organization's interests or business. If the organization were a financial institution, the applications likely would include accounting and banking operations. If the organization were a research laboratory, the applications would include capabilities for developing and manipulating files of data. If the organization were a telecommunication carrier, the applications would include all of the operations required to provide high-quality, reliable services to customers at reasonable costs. Management of the application (sub)system would be required to coordinate and control the various (perhaps, many) applications.

Interactions between applications, regardless of location, would be supported by the **distributed, processing-support (sub)system**. This support could be direct for collocated applications, as indicated by connection "a" between applications 1 and 2. Or, the support could require use of the communication (sub)system for applications at different locations, as indicated by connection "b" between applications 2 and n.

The **communication (sub)system** would provide communication facilities for applications at different locations, usually based on specific network architectures. Management of the communication (sub)system is the process that Böhm and Ullman (1989) identify, conceptually, to be network management. Network architectures of such communication (sub)systems and their associated network management systems, as well as the protocols used in exchanging the

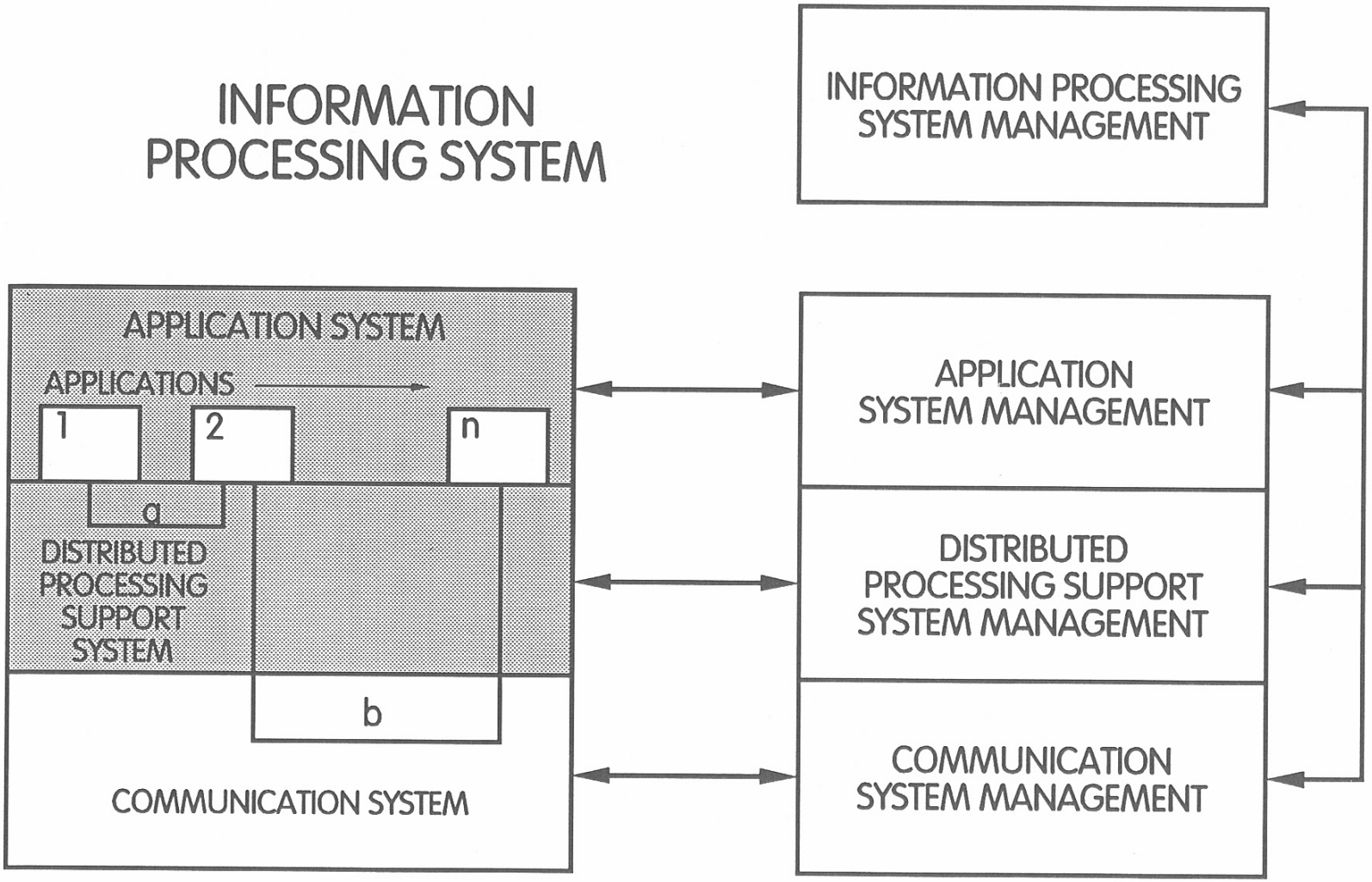


Figure 5. Conceptual structure for an information-processing system (Böhm and Ullmann, 1989).

information that is essential for doing network management, are being developed and refined by standards organizations. These network management standards efforts are discussed in Section 3.

Network managers would view networks such as those illustrated in Figures 1, 2, and 3 as being many network elements connected by some defined transmission capacity that collectively provide the desired telecommunication services, i.e., a domain of objects that they would want to manage. From a fundamental management perspective, however, the network could be considered to be a collection of managed elements (MEs) that may be divided into two classes—passive and active (Böhm and Ullmann, 1989 and Feridun et al., 1988). The passive managed elements could not be managed remotely. Such entities might include simple devices such as cables, dumb modems, and terminals or complex systems such as some PABXs that can only be managed locally. The active managed elements would include such items as intelligent modems, PABX networks, or protocol converters with internal management capabilities that enable them to be managed remotely using communication links. The capability that enables one to manage these elements may be defined as managed element management (MEM). Such capability must be suitable for monitoring and controlling all the intelligent devices and complex systems that comprise the network. Figure 6 shows a hierarchial management perspective for a network such as the one illustrated in Figure 2 (this and other management perspectives are discussed in Section 2.3).

Network management, in the context of this discussion that emphasizes the management perspective, is management of the managed elements, a process that may be performed by a network management center. For example, Figure 6 shows a network management center (NMC) that is controlling three MEM capabilities:

- a common-protocol capability for managing the 1...m managed elements in the PABX or private network
- a second, common-protocol capability for managing the 1...n managed elements in the ISDN network (that may be an ISDN island)
- a third, common-protocol capability for managing the 1...p managed elements in the Centrex or public network.

We now turn to discussion of the functions that need to be performed through the process of network management. In this discussion of functionality, several somewhat different

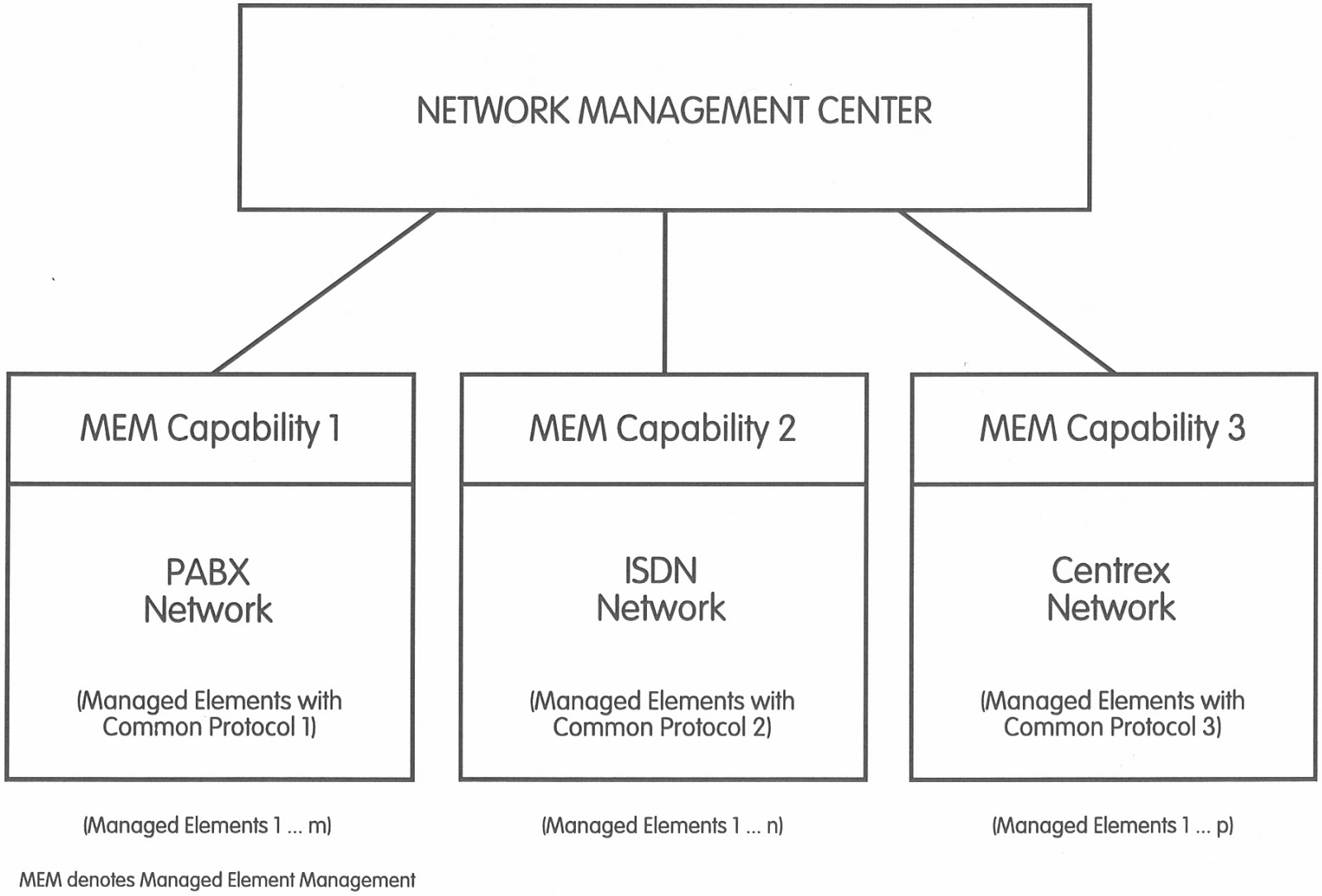


Figure 6. A user's network such as illustrated in Figure 2 from a hierarchial management perspective.

perceptions of network management are revealed. These differences reflect a refinement in understanding necessary functionality as the network management discipline has been evolving, differences associated with data-services users versus voice-services users, and differences associated with users' versus carriers' perspectives.

Earlier, in Section 2.1, we noted that Valovic (1987) has suggested three basic functional areas that relate to network management, namely monitoring and control, administration, and planning and design. Somewhat different expectations of network management tend to be held by users (or organizations, and the communications managers that represent these users) and the local and inter-exchange carriers that provide services for the users.

Some of the functions that users generally require in network management, as defined by Pyykkonen (1989), are identified in Figure 7. He notes that all of these functions are related to both physical and logical network management, but in practice, many of the functions are viewed as either physical or logical (but not both), largely due to the different views of voice and data (or management-information systems—MIS) users. Another view of network management functional categories (Caruso, 1990), that is quite complementary to Pyykkonen's view, is shown in Table 1. Each of these views presents eight functions or functional categories. One begins to see common functional areas that are included in each of these lists.

In recent development by a European telecommunications carrier of a capability for comprehensive, integrated network management, seven functional categories have been used to encompass the variety of communications management functions and services that are provided (Willetts, 1991). These categories and a brief description of each are shown in Table 2.

The Bellcore Network Management Handbook (1989) notes that "network management is responsible for supervising the performance of the network and controlling the flow of traffic ... to obtain the maximum use of network capacity." This responsibility is defined further to include the following seven specific functions:

- Monitor the flow of traffic in the network on a real-time basis.
- Collect and analyze network performance data.
- Identify abnormal network situations.
- Investigate and determine the reasons for network traffic problems.

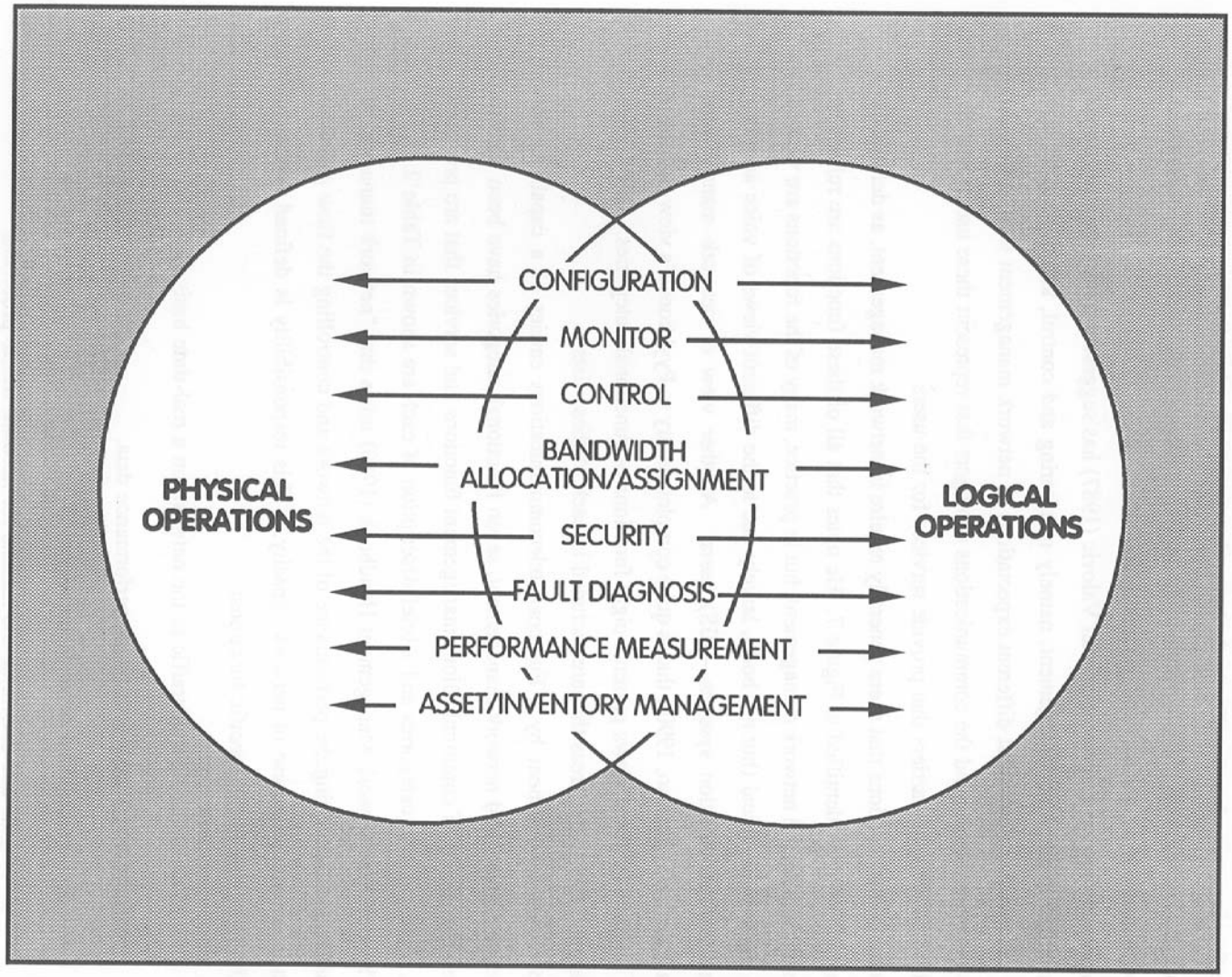


Figure 7. Functions, involving both physical and logical network operations, that users generally require in network management (Pyykkonen, 1989).

Table 1. Network Management Functional Categories Suggested by Caruso (1990)

CATEGORY	**EXAMPLES**
Fault Management	Fault detection, trouble reports.
Performance Management	Performance monitoring, alerts.
Configuration Management	Network topology database, band-width allocation, routing changes.
Accounting Management	Traffic usage statistics, billing reports.
Security Management	Secured access, intrusion detection/recovery.
Capacity Management	Forecasting, engineering.
Provisioning Management	Service ordering/tracking, pre-service testing.
Administration Management	Customer-controllable service profiles, management reports.

Table 2. Network Management Functional Categories Selected by a European Telecommunications Carrier (Willets, 1991)

Event management: deals with events occurring on the network (such as alarms) and the processes required to cope with them.
Performance management: ensures that the network is tuned to achieve optimum response times, utilization, and loading patterns.
Configuration management: covers how resources are configured into complete networks and includes disaster routing and provision for changes and expansion of the network.
Resource management: embraces the physical and logical construction of the network.
Financial management: deals with billing and costing, capital plant depreciation, and invoice reconciliation.
Access and security management: covers who is allowed to do what on the network and when.
Planning and design management: includes the series of functions required to plan new networks or extensions to existing networks, optimal routings and loadings, and fall-back strategies.

- Activate network controls or other corrective actions.

- Participate in joint planning sessions with inter-exchange carriers, local exchange carriers, and other telephone companies, and exchange information on matters of common interest.

- Coordinate activities with facility and switching system maintenance personnel to minimize the impact of outages.

Essentially, the sixteen sections of the Bellcore Handbook are detailed descriptions of these network management functions, with at least one section devoted to each function.

In the study performed by Linfield and Nesenbergs (1985), they applied the concept of telephone company operations (that is defined and discussed extensively by Rey, 1983) and the Bellcore concept of network management (Bellcore, 1989) to their discussion of Administration, Operations, and Maintenance and Network Management (AO&M/NM). Their study identifies and describes seven functional network operations as shown in Table 3. Most of these functions fall within the scope of network management presented in this report.

Many organizations are working on the development of standards for network management, and Section 3 presents a comprehensive discussion of that topic. Without providing the detailed, supporting information here, suffice it to note that (at the highest organizational levels) the Internet Activities Board (IAB)[15], the American National Standards Institute

[15] The IAB, through the work of its various subsidiary organizations, has developed the Internet suite of protocols for data communication and the associated Simple Network Management Protocol (SNMP) for network management. *The Simple Book, An Introduction to Management of TCP/IP-based Internets* (Rose, 1991) provides a thorough description of SNMP.

Table 3. Functional Examples of Telephone Network Operations Described by Linfield and Nesenbergs (1985)

OPERATION . . . . . TYPICAL TIME SCALE DESCRIPTIVE SYNOPSIS
Network Management (NM) . . . . . In Near-Real Time Controls overload by alternate routing and reassignment of traffic to already-installed equipments. If local, NM is the same as technical control.
Network Administration . . . . . Hourly - Daily Monitors traffic, keeps busy hour (BH) statistics, flags office (switch) degradations, plans and executes line/trunk assignments. Initiates installation requests.
Operator Administration . . . . . Daily - Monthly Forecasts and provides operator service forces necessary for each hour, half hour, and if need be for each quarter hour of the day.
Long-Range Planning . . . . . Up to 20 years Establishes most economic network growth and replacement strategies.
Network Design . . . . . Within 5 years Estimates where, when, and how much of specific network elements will be needed.
Implementation . . . . . From Days to Years Makes stress-dependent (changes) ASAP and slower planned economical changes, field construction, testing, and dismantling.
Maintenance . . . . . Continuous, Varied Pace Repair, replacement, diagnostic testing, sometimes routine, otherwise under stress.

(ANSI)[16], the ISO in conjunction with the ISO/IEC[17], and the International Telegraph and Telephone Consultative Committee[18] are the leading organizations.

However, a study performed by the National Institute of Standards and Technology (NIST) (Aronoff et al., 1989) to determine functional requirements in the management of networks based on open systems interconnection standards asserts that a distinction must be made between network management, as commonly understood in the telecommunications industry, and the "management of OSI-based networks." These authors conclude, however, that while distinctions must be made, they believe that OSI management can be applied to the management of telecommunication networks beyond the focus of OSI management standardization and that such application is, in fact, being made in the United States (U.S.) to telephony elements by the American National Standards Institute in work within Technical Subcommittee (SC) T1M1. (See Section 3 for additional discussion of this specific point.)

There is at this time no generally-accepted, theoretical or practical, complete implementation of standards for network management. However, functional areas have been defined (ISO/IEC Standard 7498-4, 1989) that are widely accepted. Within the functional areas, numerous specific management functions also have been defined[19]. The five functional areas are shown in Table 4 with brief, paraphrased statements to describe what each area includes. (More thorough discussion and definition of these functional areas is included in Section 3.

[16] The work of ANSI is developing network management standards is conducted by a Technical Subcommittee of Committee T1 known as T1M1. That Subcommittee is responsible for developing standards relating to internetwork operations, administration, maintenance, and provisioning of telecommunications networks. At the end of 1991 there were 18 draft standards either completed or in the process of being approved. There were an additional 10 draft standards under development in T1M1.

[17] The International Organization for Standardization (ISO) in conjunction with the International Electrotechnical Commission (IEC) have developed for information processing systems the Basic Reference Model for Open Systems Interconnection (OSI) (ISO, 1984). The framework for OSI Management is defined in Part 4 of the Basic Reference Model Standard (ISO/IEC, 1989).

[18] The results of work and agreements within the CCITT are contained in Recommendation X.200 (CCITT, 1989e) for open systems interconnection, in Recommendation E.410 (CCITT, 1989b) for international network management, and in Recommendation M.30 (CCITT, 1989d) for a telecommunications management network.

[19] For example, the OSI Network Management Forum (NMF) is following the ISO/IEC and CCITT standards in developing specifications for network management implementations (OSI/Network Management Forum, 1990), e.g., interoperable interface protocols, management services, a framework for modeling the communications network for management purposes, the architectural framework of interoperable network management agreements, etc.

Table 4. Network Management Functional Areas that are Widely Accepted by Users, Telecommunication Service Providers, and Standards-Making Organizations

Fault management: responsibility for and actions to detect, isolate, and control abnormal network behavior, such as excessive line outages (**what** "is the network doing?).
Accounting management: responsibility for and actions to collect and process data related to resource consumption in the network (**when** is the network used?).
Configuration management: responsibility for and actions to detect and control the state of the network for both logical and physical configurations (**where** is everything in the network?).
Performance management: responsibility for and actions to control and analyze the throughput and error rate of the network, including historical information (**how** is the network doing?).
Security management: responsibility for and actions to control access to network resources through the use of authentication techniques and authorization policies (**who** can use the network?).

Returning to our development of the management perspective for network management, we now expand the discussion of managed elements and relations between them (discussed earlier in this section and illustrated initially in Figure 6). A simple network is illustrated in Figure 8. This illustration, selected as a "cut" through the network illustrated in Figure 1, shows only a workstation and modem at one node connected, through a gateway and LAN, to a host computer at the other node. In reality, the network is composed of physical components (e.g., hardware devices, cables, etc.) and logical components (e.g., various software-defined services provided by the network). Each of these physical and logical components may be represented as a managed element, and the relationships between components may be represented as relationships between the managed elements. These concepts are illustrated in the simple network depicted in Figure 8. Each managed element, then, may be described using parameters, such as name, state, physical location, last maintenance date, etc., that collectively will comprise a database that describes the entire network. We have, in fact, just described the configuration management functional area defined in Table 4. The full representation of all managed elements, their relationships, and their descriptive parameters become a model of the network's managed objects—the configuration model and associated configuration database.

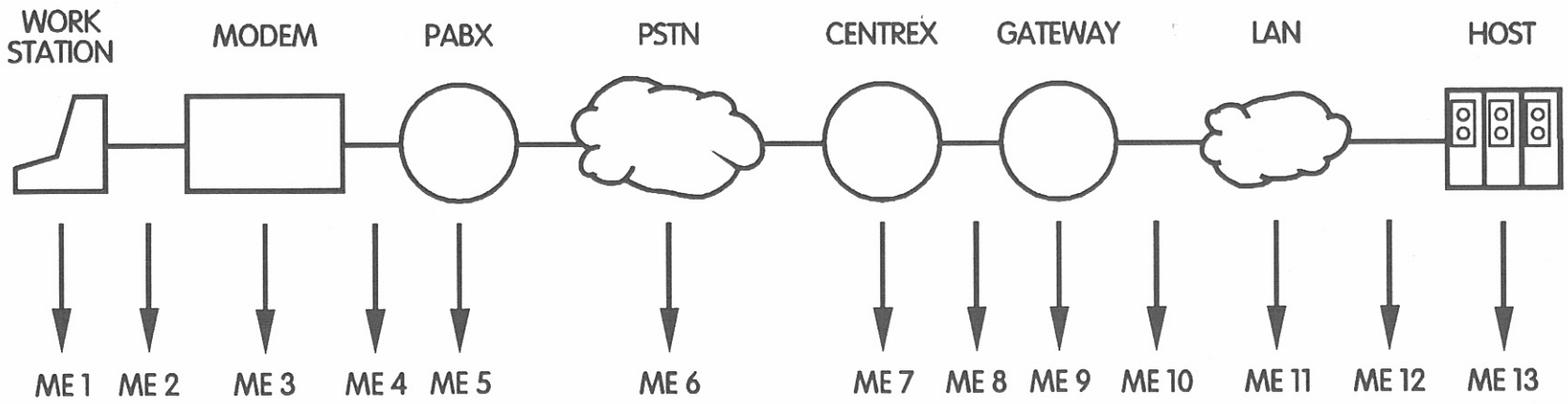


Figure 8. A simple, conceptual network, extracted from the user's network shown in Figure 3, illustrating the concept of managed elements.

We have noted that there are several possible approaches to management of the managed elements, or generic network management. The network configuration model just described must be suitable to support any of these approaches or architectures for network management. That is the subject of discussion in the next sub-section.

2.3 Approaches for Designing Network Management

A broad and very general definition for **network** is given in Section 1. The reality is that in practice many different types of telecommunication networks must interoperate and be managed for these networks to provide efficient and effective telecommunication services. The various types of networks (which may be public and private, national and international) likely will include voice networks; computer networks, such as packet-data networks, LANs, WANs, etc.; and networks for a variety of video services. In general, the communications resources of a business or organization include much more than just the physical and logical network of circuits and switches. Therefore, we use the term network management to describe the broader notion of managing all of the communication resources.

The introductory material for Section 2 gives some early, general-perspective information about network management. The historical reality, however, has been that each of the various types of networks noted above likely was established using systems (hardware and software) from a wide variety of developers and implementors, each with its own network management system (or capability). Interoperation[20] between the many individual network management capabilities now is essential, however, if overall effectiveness and efficiency are to be realized in managing and using the network. Managing these networks is more than a technical problem, however; the environment for managing telecommunication networks is, in fact, a combination of human, social, organizational, and technological components (or factors). Therefore, management of these networks to provide efficient and effective services must involve a combination of human, software, and hardware resources.

[20] Interoperation (a topic unto itself) of network management capabilities is the goal of proponents for open systems and the specific objective of the many network management standards organizations that are identified and discussed in Section 3. The concept of interoperation (or open systems) is that one tool (or set of tools that work together) can be used to manage all of the communication resources of a business or organization. Such capability often is referred to as integrated network management. (See, for example, Joseph and Muralidhar, 1990.)

As discussed above, the communications resources provided by telecommunications earners or other suppliers and used by businesses and other organizations generally are complex and heterogeneous. But, as noted by Joseph and Muralidhar (1990), these resources tend to fit into two main categories: resources that provide **interfacility** networks, such as circuit- and packet-switched telecommunications networks; and resources that provide **intrafacility** networks, such as the various forms of local area networks. The tools available today for managing networks in each of these two categories are quite different. For example, tools for managing interfacility networks focus on managing the physical and logical networks and sub-networks that are made-up of circuits, switches, and trunks (Aronoff et al., 1989), whereas, tools for managing intrafacility networks are very diverse, ranging from relatively simple modem managers to relatively complex LAN management systems. From the perspective of user control, relatively less effort is being devoted to development of tools for interfacility network management, and relatively more effort is being devoted to development of tools for intrafacility network management. The availability of user-controlled tools for managing networks in each of these categories is about proportional to the development effort in each. And, the network that needs to be managed typically is a complex mix of resources and services—a combination of many interfacility and intrafacility networks and sub-networks for which users feel there needs to be a common network management capability.

Basically, there are three main approaches that may be followed to develop and provide this common network management capability. These are the centralized approach illustrated in Figure 9, the distributed approach illustrated in Figure 10, and the hierarchical approach illustrated in Figure 11. There also would be various combinations of these approaches that could be used.

In the centralized approach (Figure 9), all management entities are connected directly to the network management center which carries out all management functions. That is to say, the management entities have little or no inherent management capabilities, and all management data are exchanged directly between the network management center and the respective management entities, using appropriate protocols. This approach to network management tends to be the most economical to implement because a single location gathers, processes, and stores all the data required to control the network. However; the collection of data from many management entities and the distribution of control instructions throughout the network can consume significant

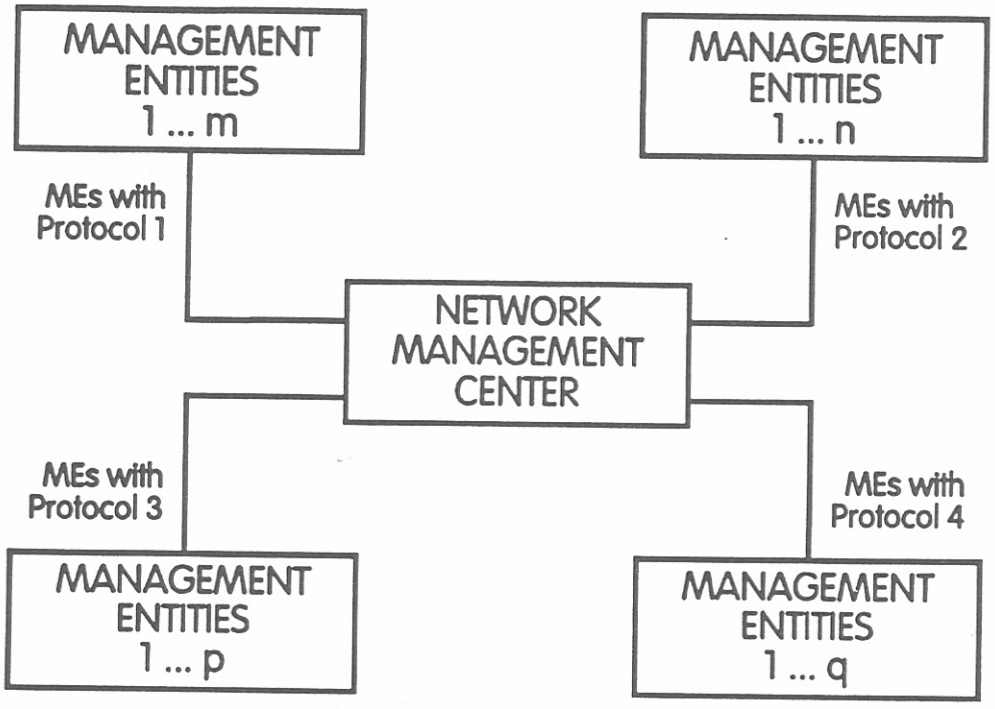


Figure 9. Centralized approach to network management.

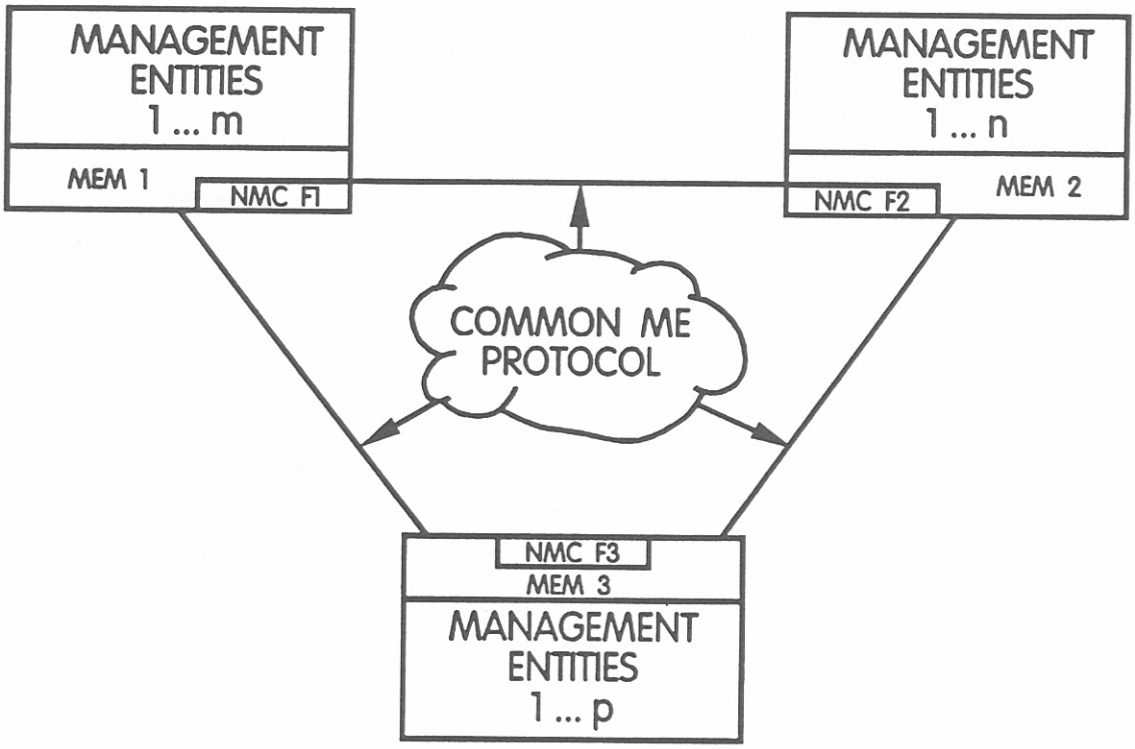


Figure 10. Distributed approach to network management.

portions of the network capacity, particularly for large networks, thus effectively reducing the network resources available for supporting the users' communications requirements. A single location for all data processing and storage also introduces a single point for failure. If the network management center fails, all management capability for the entire network is lost.

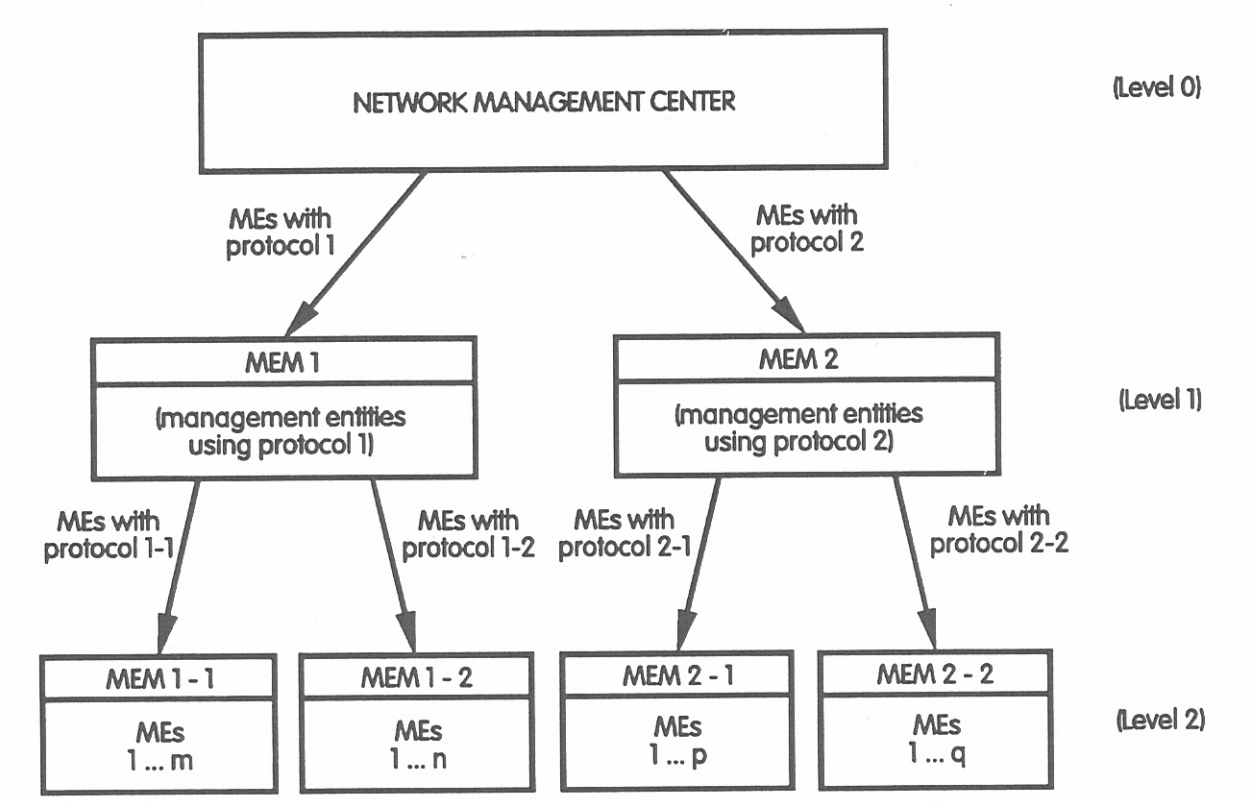


Figure 11. Hierarchical approach to network management.

In Figure 10, the network management functionality is distributed throughout the network. In this distributed approach, all MEM capabilities are interconnected, and all management entities can communicate with one another, provided the required condition of a common management protocol being used throughout the network is satisfied. (This requirement points directly to the benefit of open systems and standards for network management, features that are discussed in Section 3.) The distributed approach is more expensive than centralized network management because it requires every location to have network management capability, i.e., computer processing power and memory for storage, but there are at least two features that contribute to better performance. If one management entity manager fails, only part of the total network

management capability is impaired. Considerable management functionality still is available for the remainder of the network. Secondly, with management functionality distributed throughout the network, there is less need for large amounts of management data to be exchanged over the network. Therefore, a larger portion of the network resources is available to support the users' communications requirements.

Several levels of management functionality in the hierarchical approach are illustrated in Figure 11. All management entities have some management capability that supports the collection and issuance of management information (or data). The network management center manages the next lower level of MEM capabilities and that level may manage still another, lower level of MEM capabilities. If the network management center fails, the highest level of management functionality is lost, but the next lower level of management functionality can take over to keep the network in operation. Some of the same advantages and disadvantages of the distributed network management approach also apply to the hierarchical approach, e.g., improved performance when compared to the centralized approach, but higher costs for implementation because of the redundant capability required for hierarchical network management.

Joseph and Muralidhar (1990) also identify three approaches to (or implementations for) network management as being centralized network management, distributed hierarchical network management, and distributed peer network management. These approaches are illustrated in Figure 12, where we see many similarities with the approaches discussed earlier and illustrated in Figures 9-11.

The different approaches to network management that have been illustrated and discussed are not exhaustive, but form the basis for many specific, network-management implementations. Some of these implementations are discussed in Section 4 where various specific and, sometimes, proprietary, network management systems are identified and discussed.

Meanwhile, the next step in describing fundamentals of network management is to consider the architecture for network management. Every organization concerned with providing or using telecommunication services should formulate its own management strategy consistent with its objectives and installed base of communication and information systems equipment. Any of the approaches discussed above, or derivatives of those basic approaches, may be followed to develop an architecture that will provide the features that are important to users and providers in their network management systems. The architecture should identify the major system

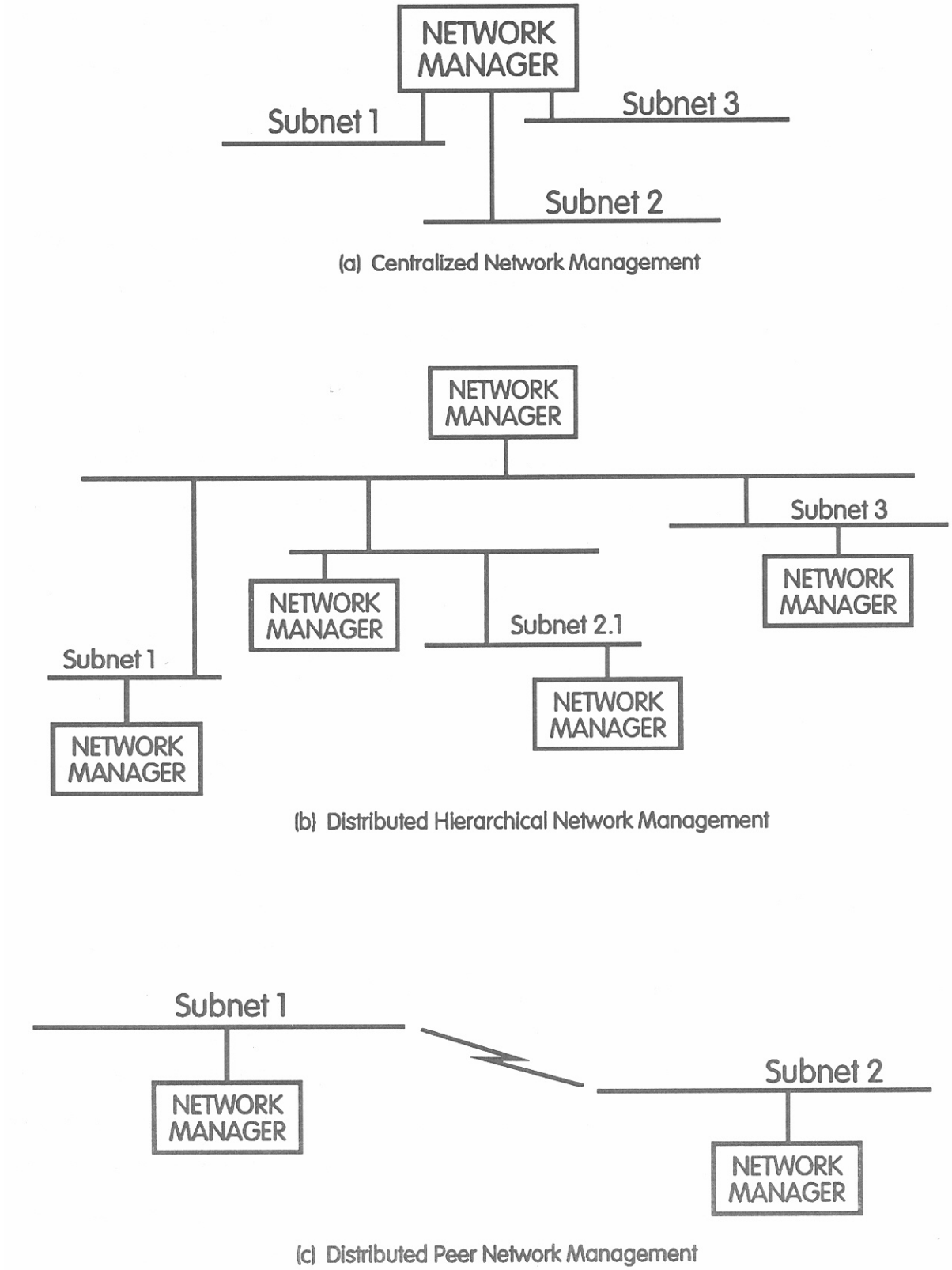


Figure 12. Possible network management implementations suggested by Joseph and Muralidhar (1990).

building blocks and specify the relationships that must exist between them so as to define a high-level framework that can be followed during detailed system design and implementation. The management architecture also should describe the organization of people, functions, and computer-support systems that will be needed to plan, operate, and administer the network and all of the network services. Some important characteristics of the architecture are that it utilize common descriptions of all the network components and capabilities and that it specify the minimum management functionality that is required in each network component to satisfy the overall management requirements. In summary, the architecture (or architectural design) becomes a way to identify and define the management functions that are needed, by applying management techniques rather than being limited to capabilities that are offered by technology available in 1991/92 or expected to become available as long as a "piece-wise approach" to network management is followed. That is to say, developing the network management architecture should be treated as a "systems problem" rather than as a "tools issue". Then, the architecture is a set of guidelines and ground rules that ensure that all of the constituent parts of the complex system will work together.

Desikan (1990) has described network management system architecture as consisting of four major components: managed objects, a management information network, a communications processor, and a manager. A conceptual illustration of this network management system architecture is illustrated in Figure 13.

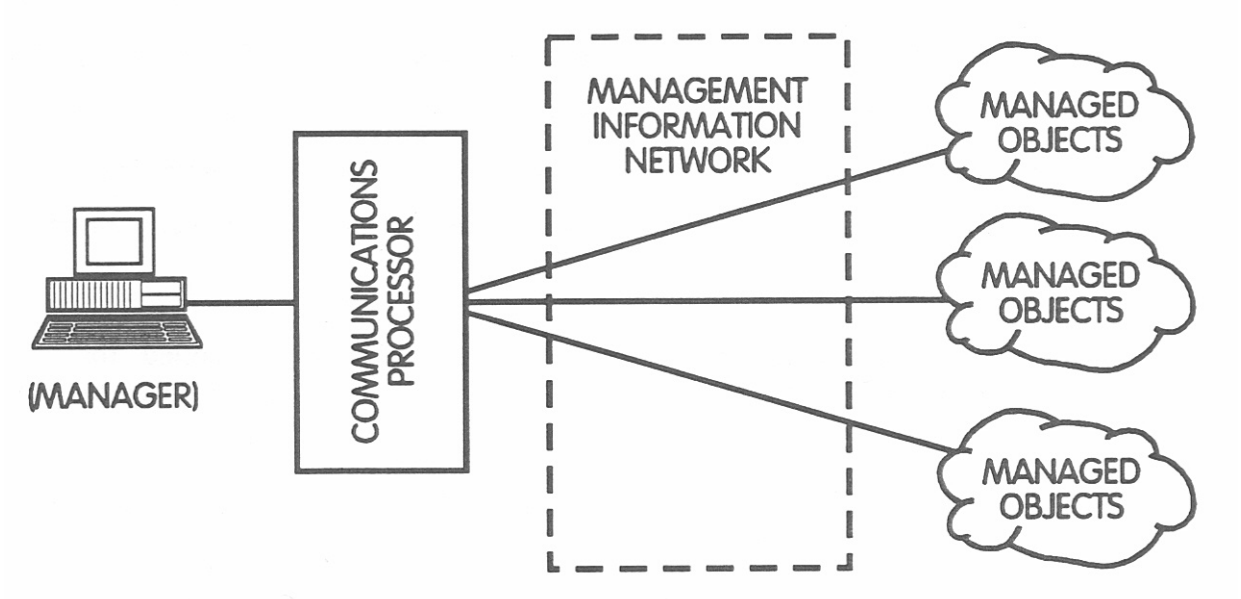


Figure 13. A conceptual illustration of network management system architecture.

Managed objects are components that generate events and reports and that are controlled by the network management system manager. Examples of managed objects include T1 multiplexers, local area network bridges and routers, matrix switches, and element management systems that are part of other network management systems.

The management information network is a data communications network that is used to transport management information, e.g., events, reports, etc., between the managed objects and the communications processor. This network may be a virtual network that is derived from the user's physical network. The TMN that has been defined by the CCITT (1989d) to support the management of telecommunications networks is an example of such a network.

A communications processor may or may not be required. When required, it multiplexes messages from the managed objects into a single data stream for transmission to the manager and provides protocol conversions that may be required between the managed objects and the manager. An ideal network management system would use a common protocol throughout the network and, therefore, not require any protocol conversion. However, many of the network management systems that are in-service and being placed into service today use proprietary protocols for exchanging information (data) between the managed objects and the manager. The management information network may have sufficient capability to perform any required protocol conversions and multiplex the messages between the managed objects and the manager.

The manager is a computer-based system that interprets information (data) from the managed objects, provides instruction (or control) responses back to the managed objects, and presents results, either graphically or in a text format, to the operator via an appropriate interface. For small networks, the manager may be a personal computer (PC); for larger networks, the manager may be a workstation, minicomputer, or main-frame computer, as appropriate.

According to Ben-Artzi et al., (1990), there are two models for network management that are used widely:

- **Polling-based management** where managed objects are polled for information of interest and this information is synchronously returned to the manager.

- **Event-based management** where managed objects asynchronously send pre-configured information of interest to the manager.

The Simple Network Management Protocol (SNMP), for Transmission Control Protocol/Internet Protocol (TCP/IP) based networks, is an example of polling-based management, whereas the Common Management Information Protocol (CMIP), for ISO/OSI-based networks, is an example of event-based management.

The functional capabilities that must be provided, regardless of the network management architecture that is used, are the capabilities discussed in Section 2.2. Today, there are no single network management systems that provide all of the functional capabilities described there or that have an architectural design to allow use of common protocols throughout the entire network (often referred to as open network architecture (ONA)). Open network architecture and full-capability, network management functionality are the general objectives of various standards organizations.

Characteristics of various network management protocols and the work being done by many standards organizations are described in Section 3. The network management systems that are in service and available to be placed in service are discussed in Section 4, along with some discussion of the efforts that are being directed to the realization of interoperation between the various systems that otherwise cannot interoperate.

2.4 Factors Influencing Development of Network Management

The concepts of network management that have been developed thus far in Section 2 are idealistic. Several factors must be recognized and taken into account as we progress from these idealistic concepts to discussing the development of standards for network management and the development and use of network management systems. These factors include

- the diversity of efforts that are being directed to the definition and development of standards for network management
- the reality that development and introduction of network management systems are evolutionary processes that began with conceptually simple objectives and systems, but are now progressing rather rapidly toward complex processes and sophisticated network management systems
- the dilemma that arises because market competition and regulations on the telecommunications market may combine, though not as an intentional plan, to discourage the development and implementation of integrated capabilities for network management.

2.4.1 Multiple Standards

Extensive information concerning standards for network management is presented in Section 3 and Appendix A. The comments that follow depend on that information for basis but are included here because they represent a significant factor that is affecting the development of network-management practices and systems.

The Internet community has for several years directed considerable effort into the development of standards for data networks and services and the management of these networks. This work has been (and continues to be) coordinated by the IAB which has two principal task forces: the Internet Engineering Task Force (IETF) and the Internet Research Task Force (IRTF). The IETF is responsible for defining architecture and protocols and for developing standards, including standards for network management, that are recommended for IAB approval. Their work has included development of the TCP/IP-based SNMP and the definition of an associated Management Information Base (MIB). Work also continues to be directed to the definition and development of a framework for common management information services (CMIS) and protocols that are compatible with the ISO/OSI-based standards. The Common Management Information Services and Protocol over TCP/IP (CMOT) is the principal network management product from this effort.

The SNMP and associated MIB are criticized by many as too limited in the capabilities offered for network management. Proponents and users of SNMP argue, however, that it is available now, it works, and it provides an adequate capability that satisfies their requirements for network management.

The international efforts in developing standards for network management are very diverse. For example, the ISO has developed and promoted such standards as CMIS and CMIP and defined an associated MIB for data networks. Much of this work (but not all) has been endorsed and adopted by the CCITT. In addition, the CCITT has defined International Network Management, for telephone service including ISDN, and the TMN, that include definitions of many management functions. Many other international and national groups, such as the OSI Network Management Forum (NMF), the Accredited Standards Committee T1 and. Technical Subcommittee T1M1, and groups accredited by the American National Standards Institute also are providing support to the development of international standards.

The international standards that are emerging are broad, not entirely consistent, and, often, too general. These characteristics of the standards cause difficulty when attempting to develop and market network management products that conform to the standards. They also foster reluctance by both users and product developers to attempt to conform with the standards, since the generality and lack of total consistency mean there is no guarantee that products from different developers/vendors will interoperate or provide exactly the same functionality. The positive side of international standards, however, is that such standards do tend to promote system interoperability and conformance to open network architecture objectives and the standards are supported widely outside of the United States. For these reasons, U.S. products in the international markets must conform with these standards to be successful. In addition, the international standards, generally speaking, have greater functional capability than most other standards, for example, the IAB or INTERNET standards. This last point is discussed more completely in Section 3.

Considerable effort is being directed by several National (United States) organizations (see Section 3.2.2) to developing network management standards. Much of their efforts have the dual objectives of developing National standards, and resolving vague and ambiguous features of international standards, and contributing to the development of international standards.

The United States Government also has become involved in developing standards for network management with issuance of the Government Network Management Profile (NIST, 1991). This profile was written because the Government has urgent needs for products to manage networks composed of multi-vendor components, and it recognizes that existing ISO/OSI based standards still are at an intermediate stage of development.

Finally, there are numerous product developers/vendors who have developed their own proprietary "standards" for the products that they market. Several of these standards have, for a time at least, been accepted by many users as de facto standards for the products used in their networks. Examples include the Systems Network Architecture (SNA) developed and used by International Business Machines Corporation (IBM), the Open View network architecture developed and used by Hewlett-Packard Company (HP), the DECNet architecture developed and used by Digital Equipment Corporation (DEC), etc. Fortunately, most of the companies that have been developing and using these proprietary, de facto standards now are attempting to achieve

compatibility and inter-operability with equipments and systems that conform with either the SNMP or CMIS/CMIP standards, or both.

2.4.2 Evolutionary Processes

We have described how the telephone company provided the earliest network management. Then, as data communications developed and opportunities to provide new services were recognized following divesture of the Bell System, the requirements and capabilities for network management also expanded. These, of course, were (and continue to be) evolutionary processes that first provided simple management for individual elements of the network. As the number and complexity of the elements increased, the requirements for and complexity of network management systems also have increased. Now, we are hearing managers and providers of networks and network services expressing their needs for comprehensive, or integrated, network management.

The development of standards for network management and inter-operability of the network management systems is an integral and essential part of these evolutionary processes for developing and marketing management products. But, a reality in the process is that increased synergy among the standards, widespread conformance with the standards, and the ultimate capability of truly integrated network management with systems inter-operability will occur only as it becomes economically viable. Users of TCP/IP and SNMP, for example, are likely to continue to request SNMP products as long as such products are the least expensive and satisfy their management requirements. Products that conform with ISO/OSI standards for interoperability and integrated network management will be developed and available to users only as developers/vendors perceive an economically-viable demand. That demand will arise only when managers recognize their existing management capabilities to be inadequate to satisfy their (increasing) requirements and such products are available at reasonable cost.

2.4.3 Market Competition and Regulation

Both favorable and unfavorable influences arise from market competition and telecommunication regulation on the development of network management standards and systems. For example, competition continually stimulates the development of new and innovative technology that benefits users with more and easier-to-use capabilities and services at competitive

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

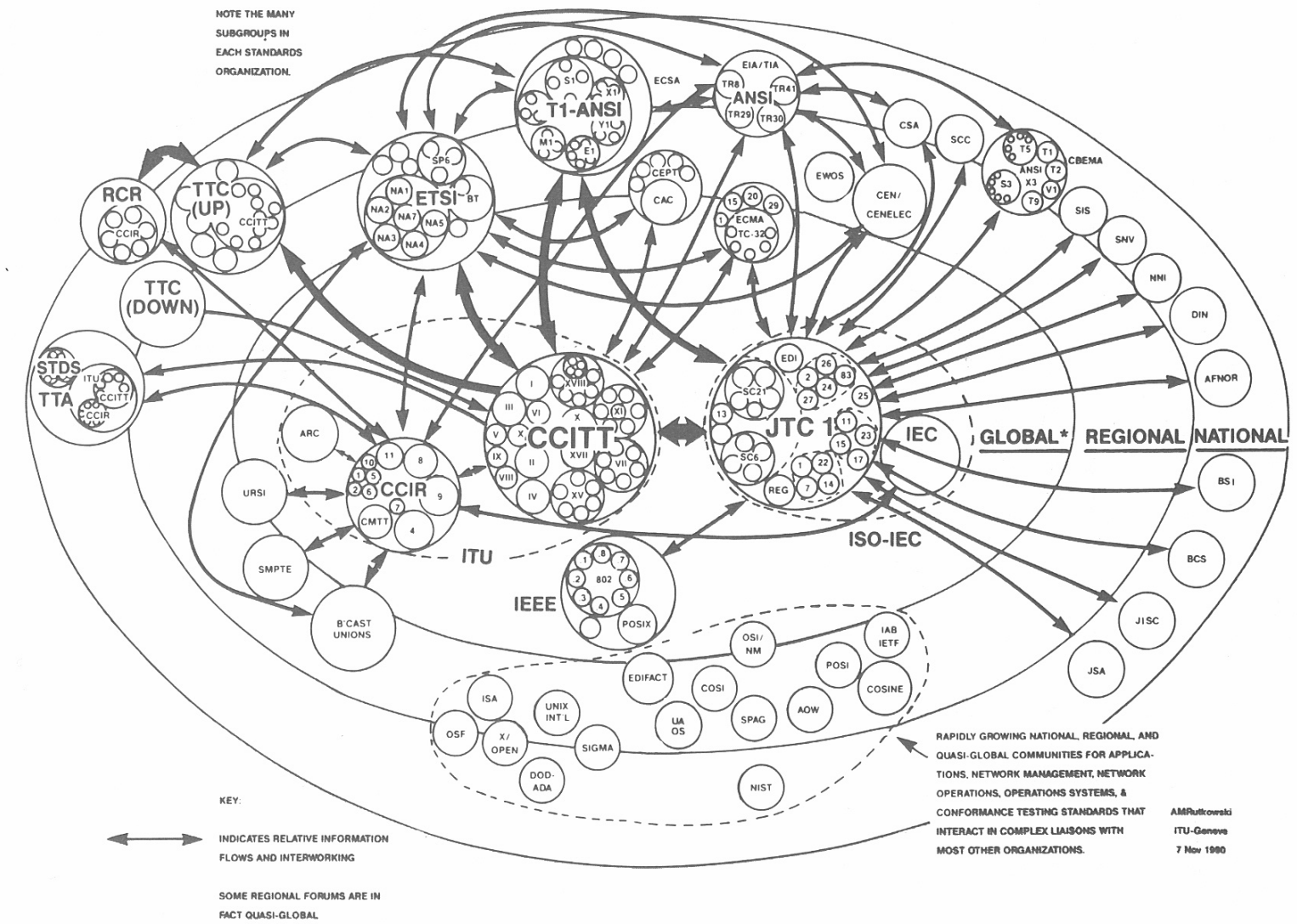


Figure 14. Global, regional, and national standards organizations (Knight, 1991).

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.

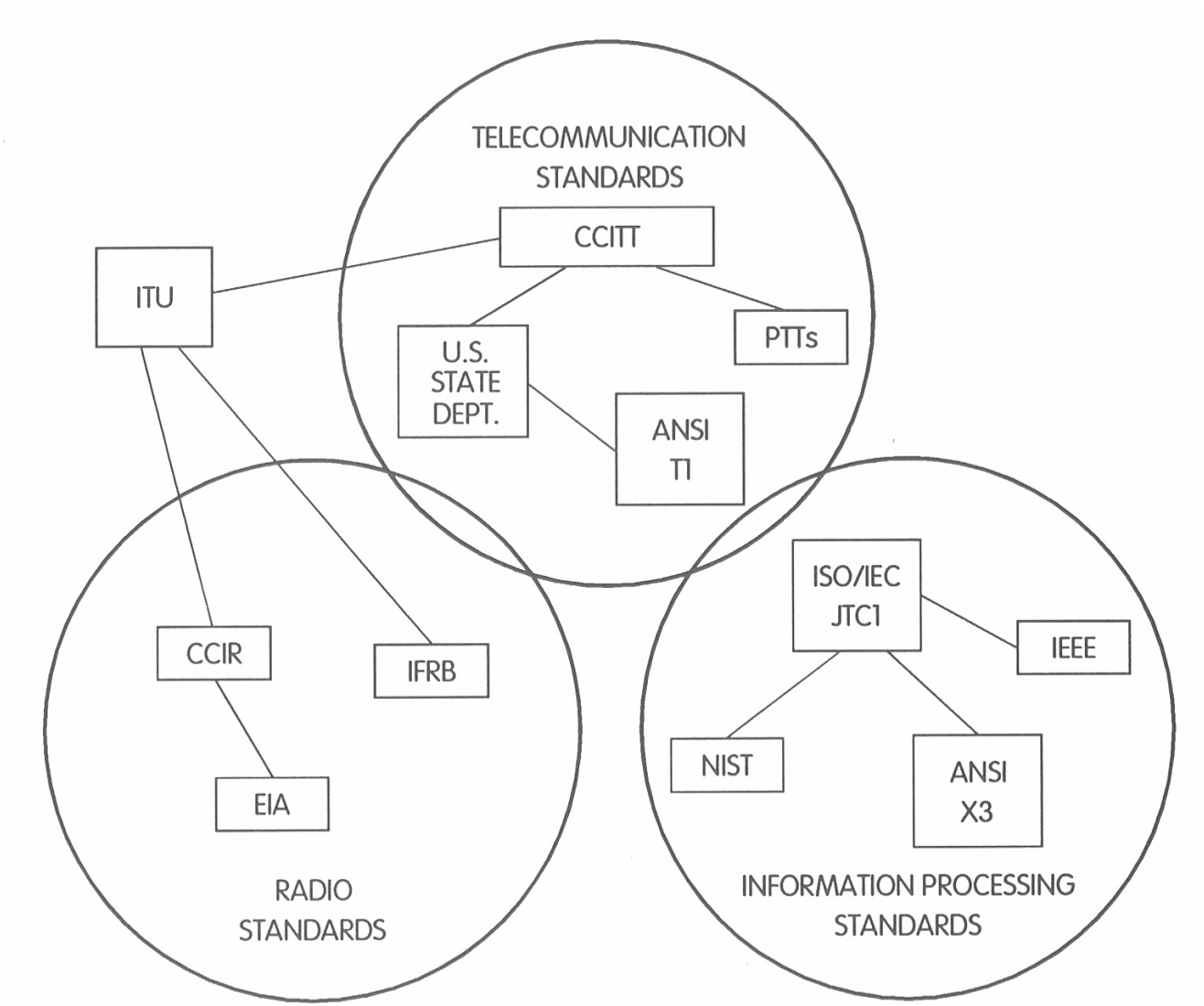


Figure 15. Major groups involved with standards for telecommunications and information processing.

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)

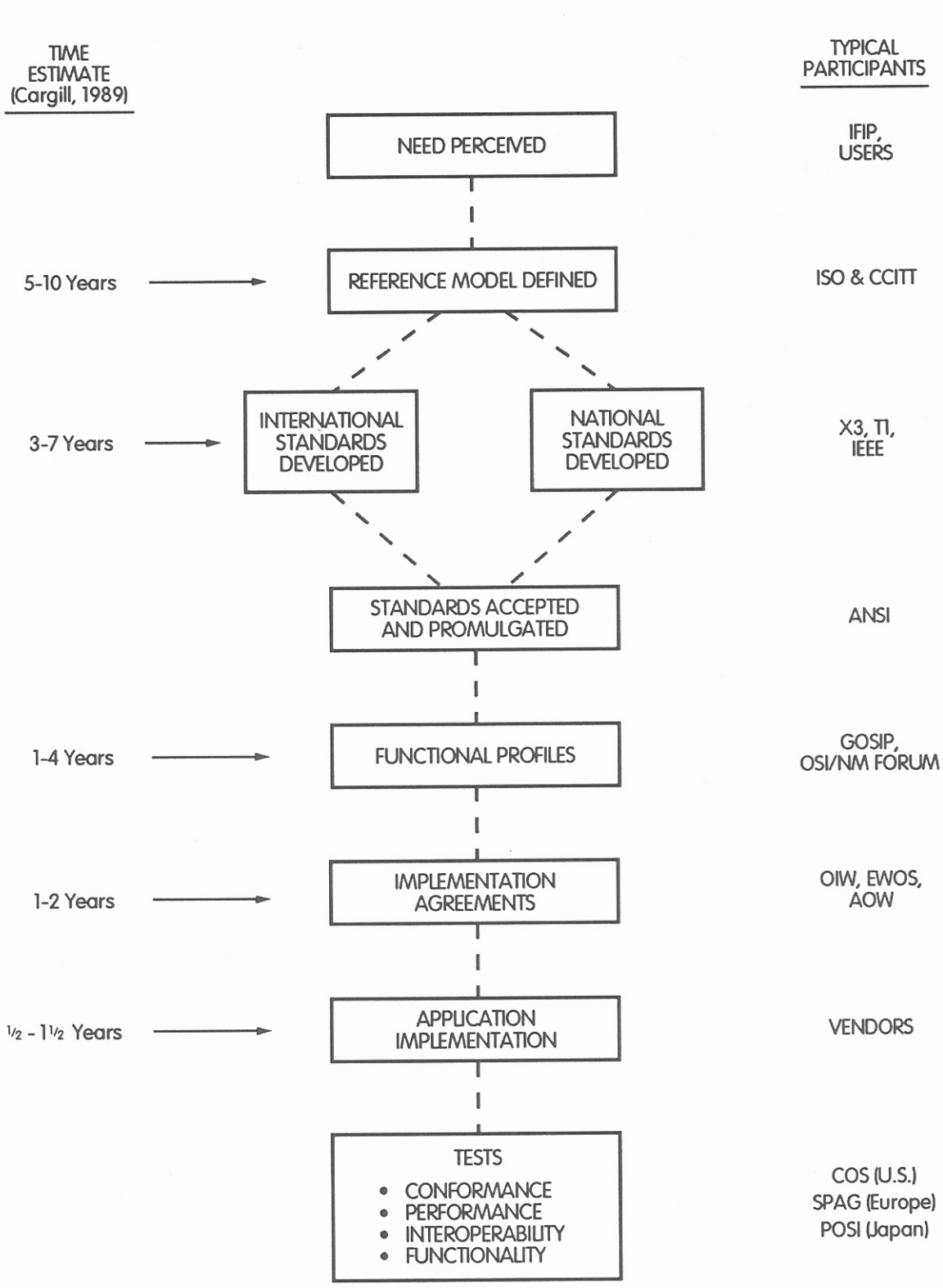


Figure 16. A model for the standards-making process.

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

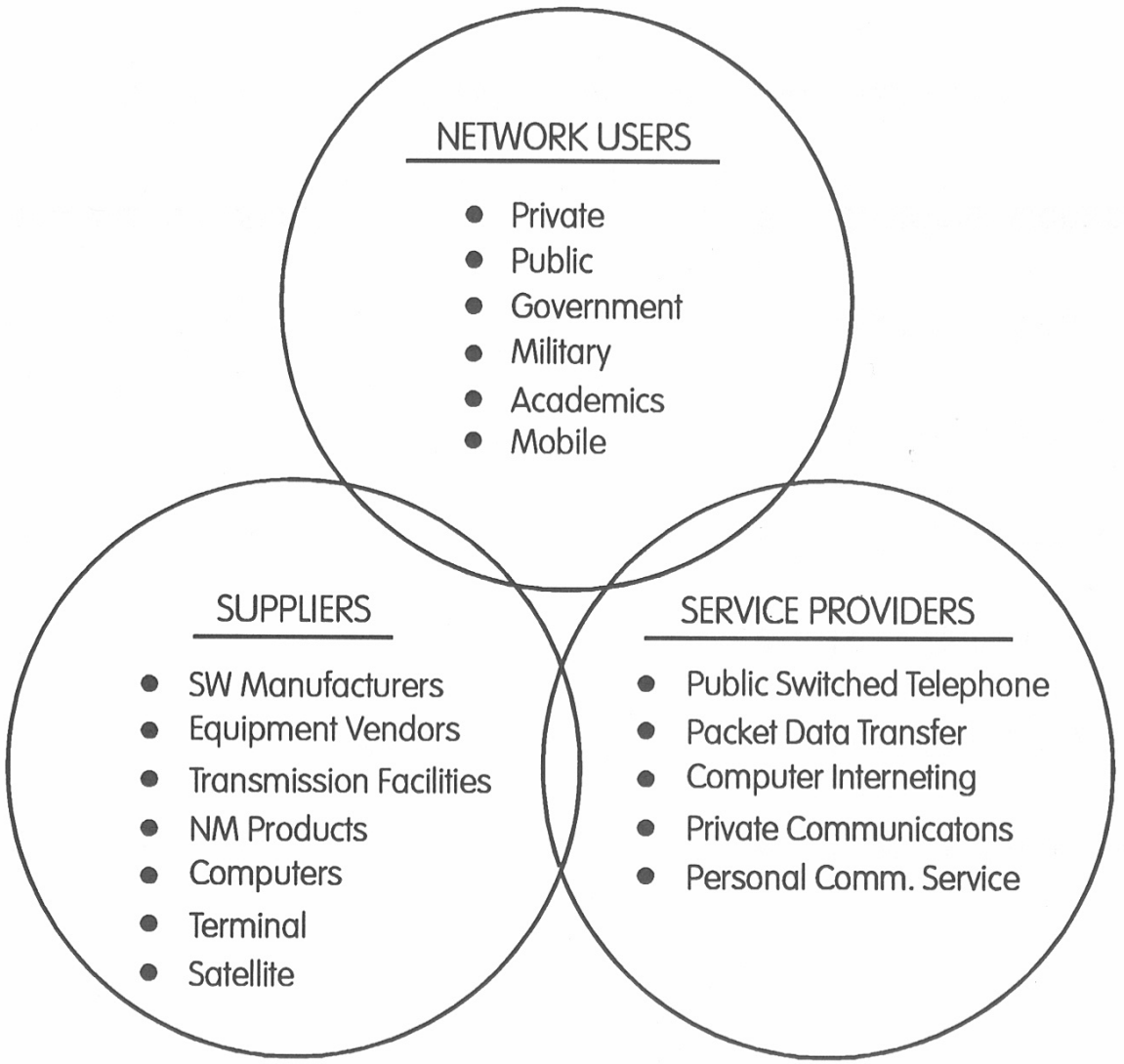


Figure 17. Major participants in the standards-making process.

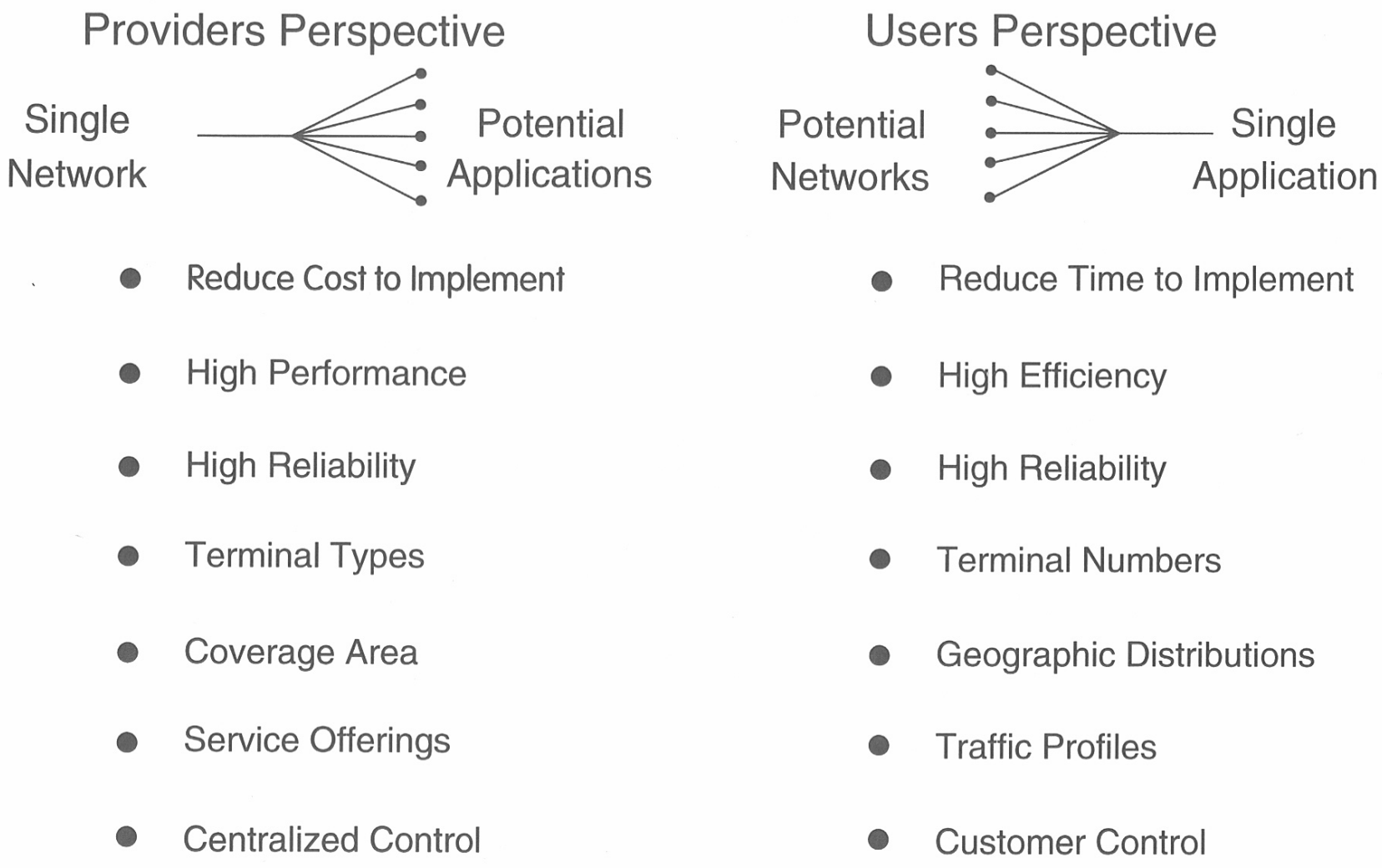


Figure 18. Critical distinctions between users' and providers' viewpoints.

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.

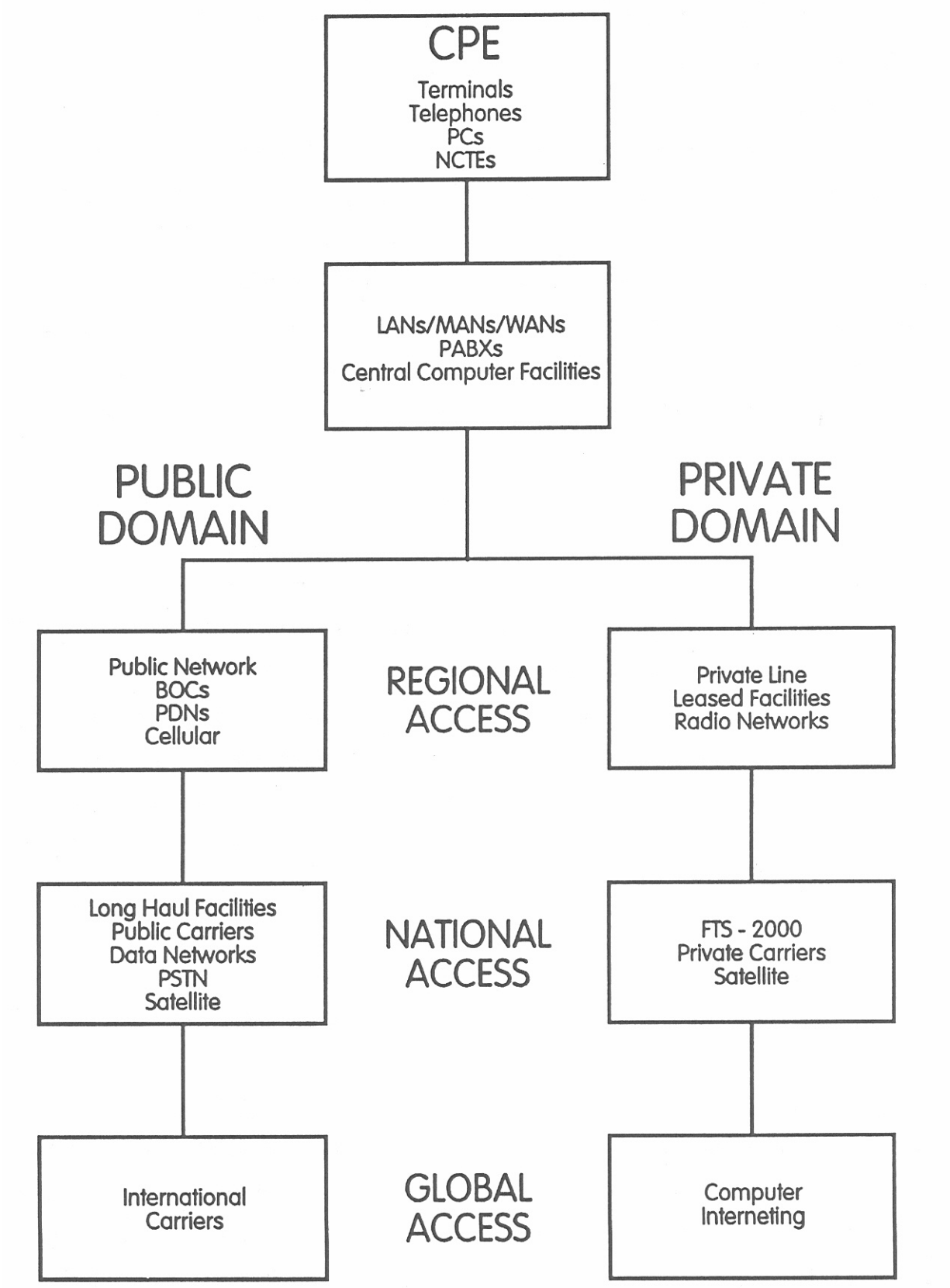


Figure 19. Domains of network management and administrative responsibilities.

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

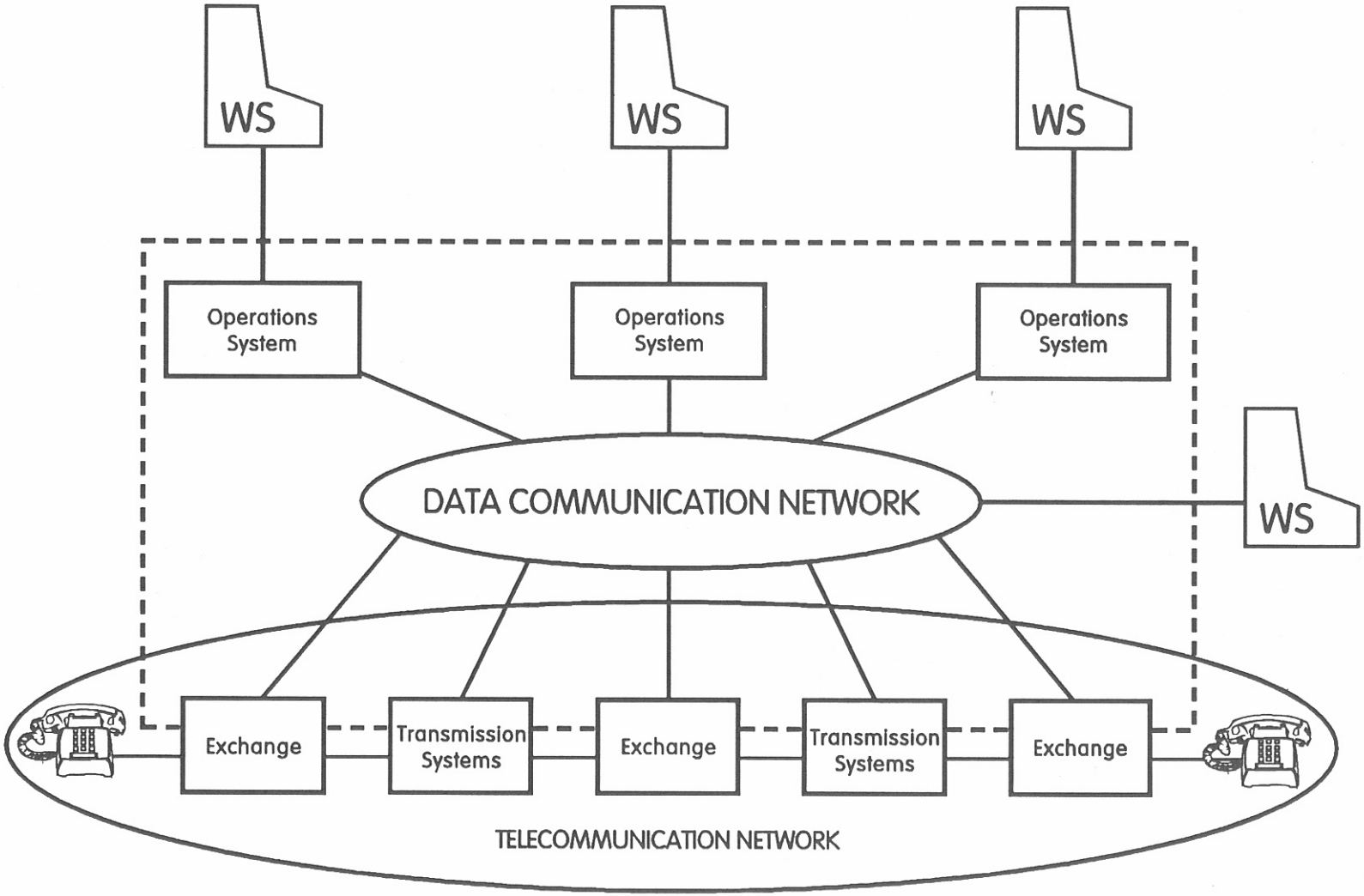


Figure 20. Relationship of TMN to a telecommunications network (CCITT, 1989d).

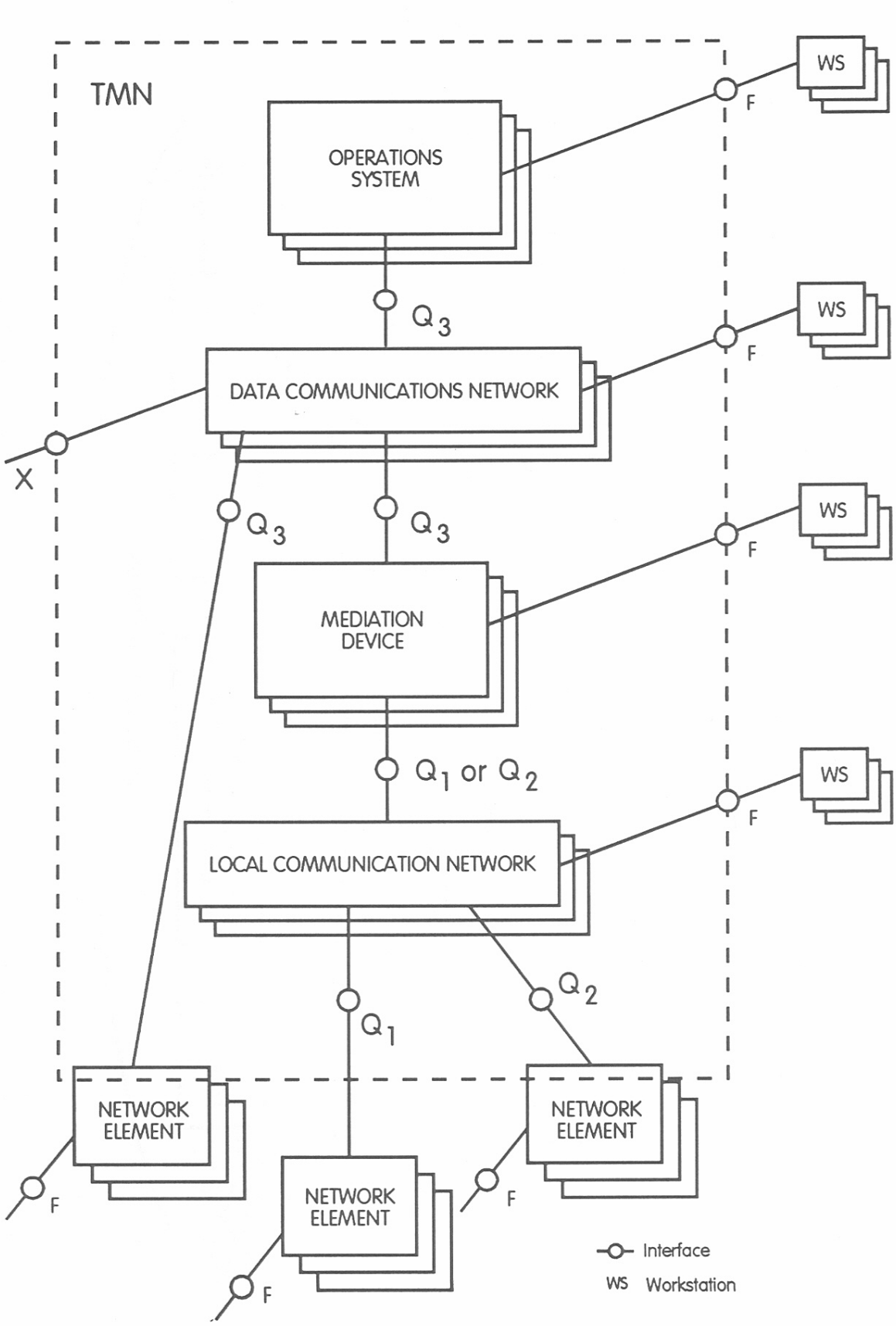


Figure 21. Physical TMN architecture (CCITT, 1989d).

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.

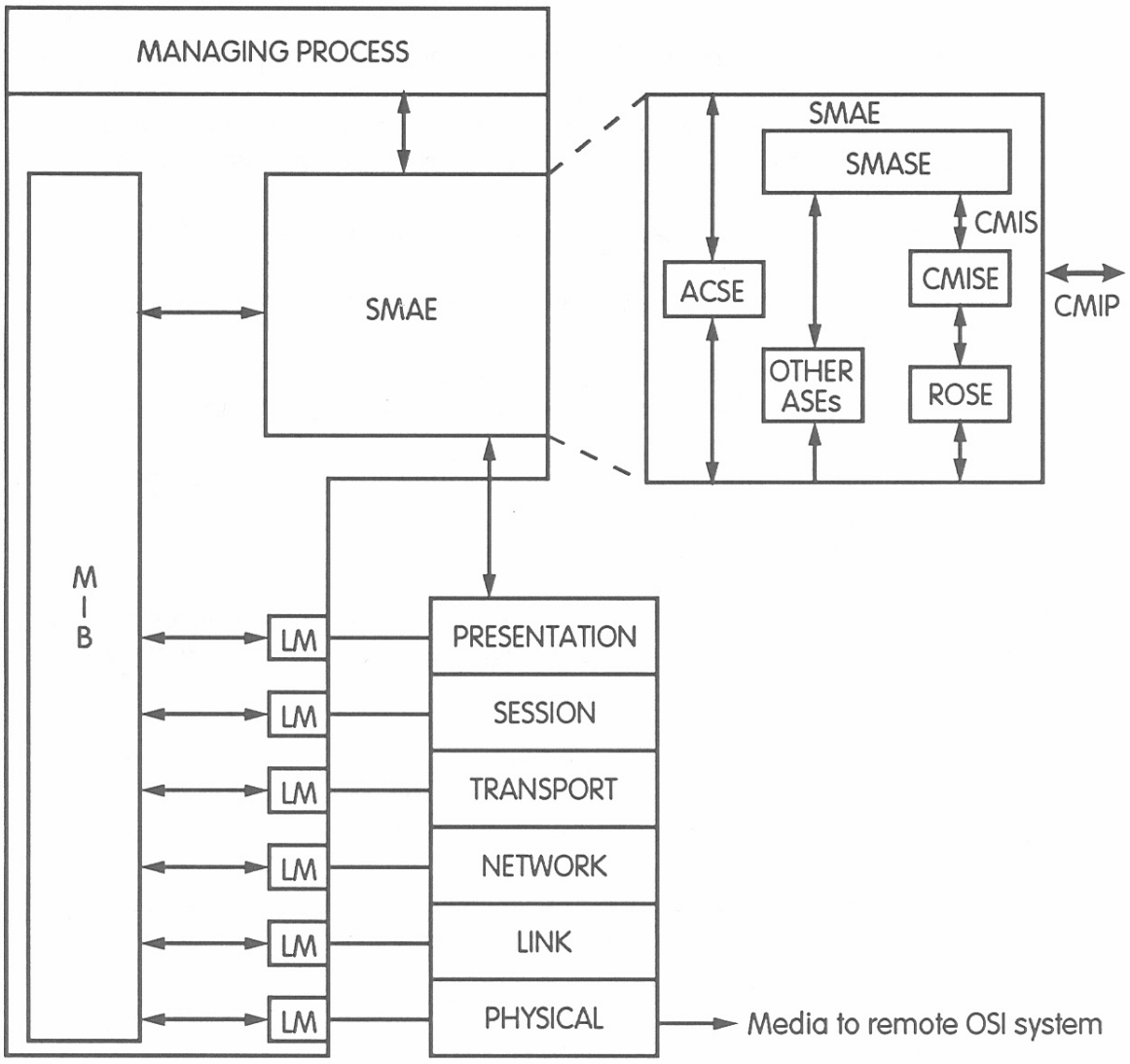


Figure 22. Architectural model of OSI management (Bartee, 1989).

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.

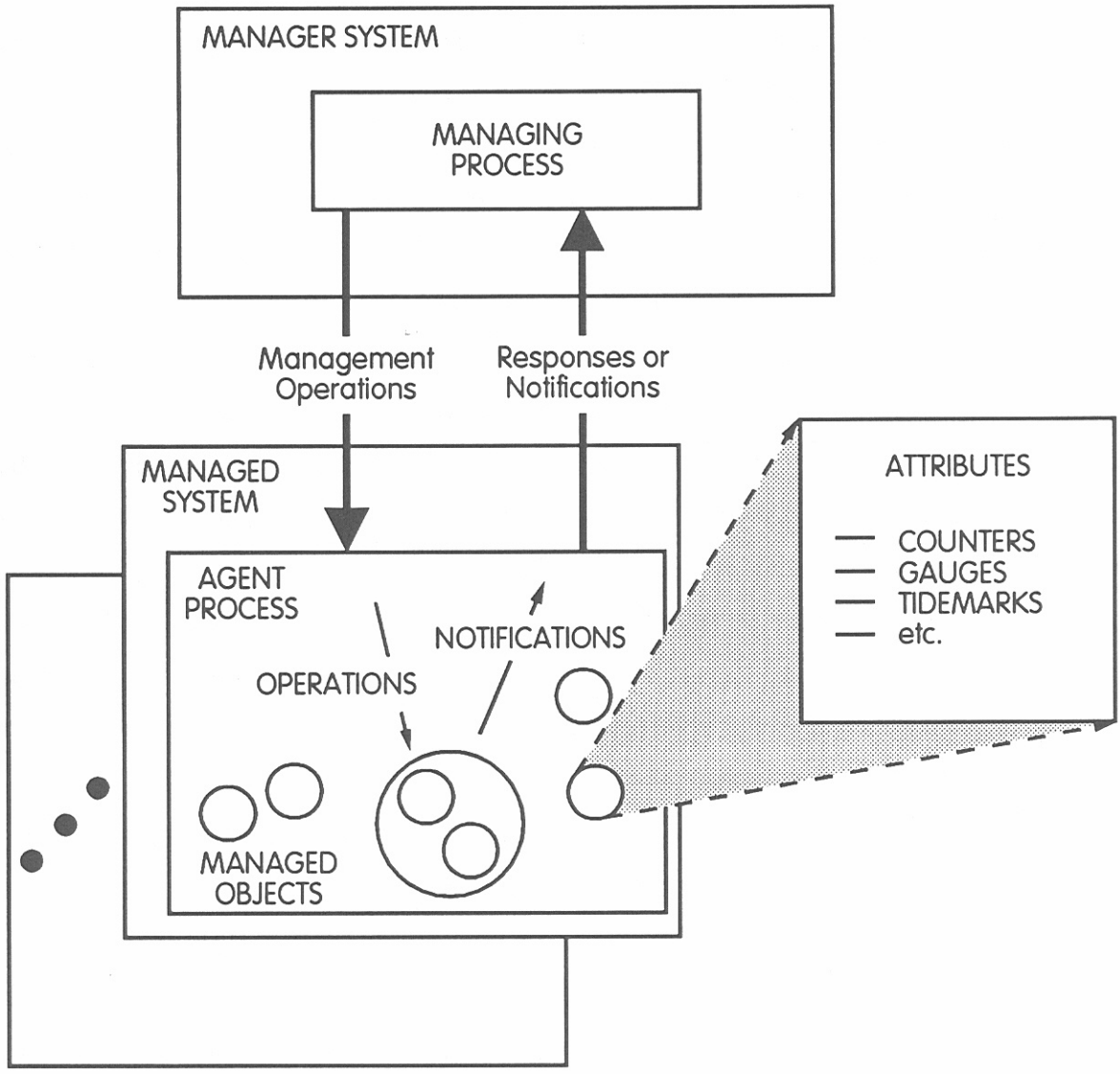


Figure 23. Basic network management framework (Bartee, 1989).

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.

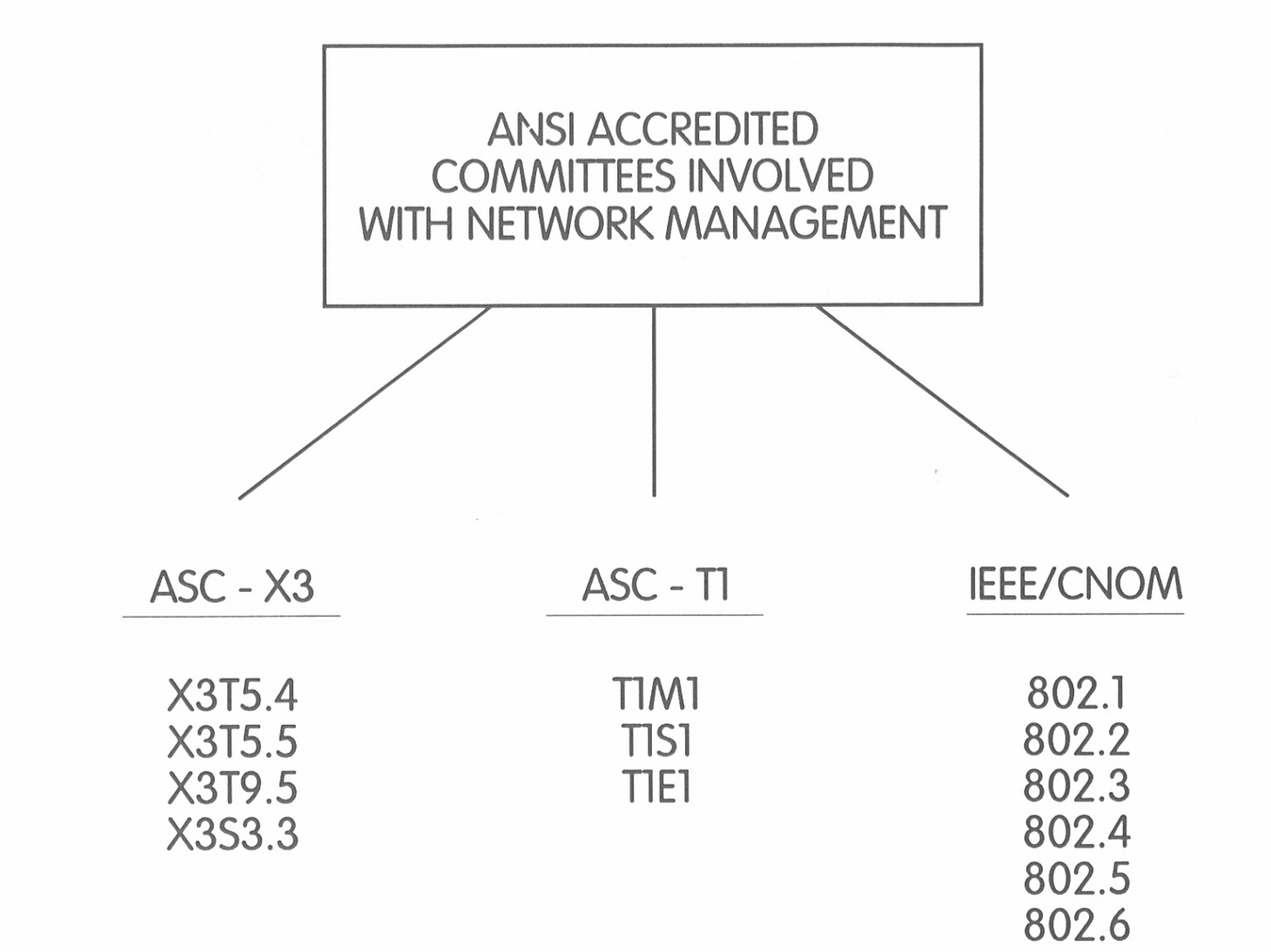


Figure 24. ANSI accredited standards committees involved with network management (as of April, 1992).

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.

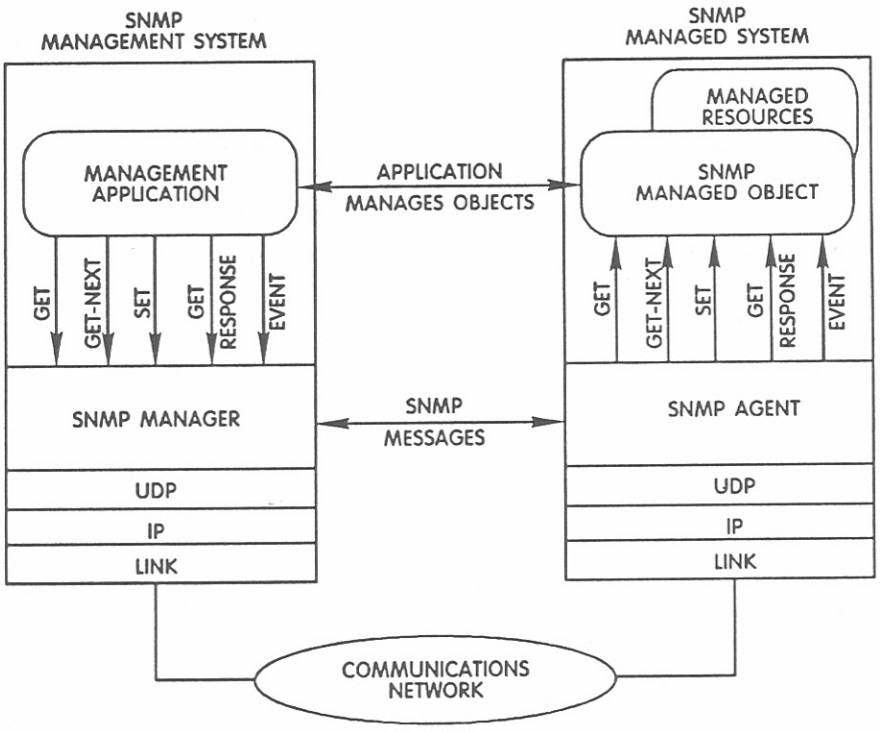
The SNMP standards work is conducted by various groups within the IETF. One group is concerned with IAs for managing asynchronously generated events and another group is concerned with protocol specifications for SNMP security management. The MID working group defines objects and provides standards for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

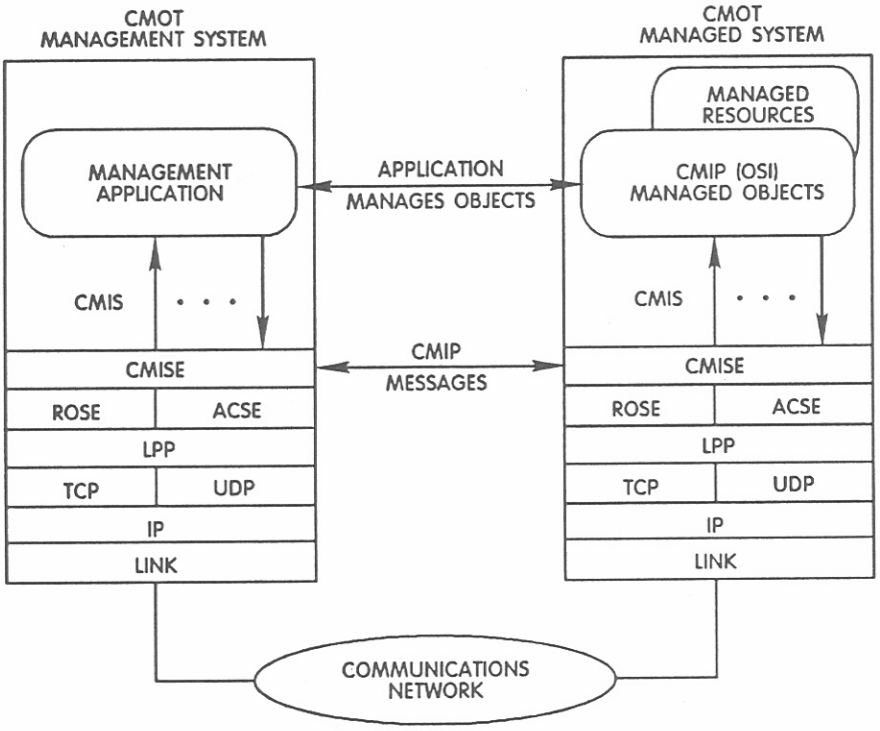
The CMOT group known as "OSI Internet Management" (OIM) working group provides CMIP-based management standards for the Internet protocols and OSI LAN/WAN portions of Internet. A Management Services Interface Group (MSI) is defining a common set of services for managing systems in the multivendor environment.

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),

Table 8. Network Management Standards Activities
(from Aronoff et al., 1989)

Management Element	Standards Group	Work Items	Status*	Estimated Completion Date
Architecture	ISO SG21/WG4	OSI Management Architecture	IS	Complete
	IEEE 802.1	LAN Layer-Management Architecture	WD	Undecided
	CCITT SG VII	Telephony Network Management Architecture	Work starting	1990
Management Communication Services and Protocols	ISO SC21/WG4 & CCITT SG VII & IAB NetMan	Common Management Information Services (CMIS) and Common Management Information Protocol (CMIP)	DIS Work starting RFC	1989-1990 1990 Complete
	IEEE 802.1	LAN Layer-Management Protocol	WD	Undecided
	IAB	Simple Network Management Protocol, a transition protocol for managing the internet before OSI's CMIP/CMIS are deployed	RFC	Complete
System Management Functions	ISO SC21/WG4 & ANSI T1M1.5 & CCITT SG VII	Configuration Management and Fault Management,	WD	Undecided
		Performance, Accounting and Security Management,	WD	1991-1993
		Common Functions such as state management, error reporting used in systems management	DP	1991

*Status is indicated as follows:

DIS: Draft International Standard
DP: Draft Proposal
IS: International Standard
RFC: Request for Comment (equivalent to standard)
WD: Working Draft

Table 8. continued

Management Element	Standards Group	Work Items	Status*	Estimated Completion Date
Managed Objects	ISO SC21/WG4 & ANSI X3T5.4	Defining structures, formats and guidelines for managed object definitions (structure of management information)	DP	1991
	ISO SC21/WG4	Defining parameters to be managed for systems (WG4: systems identification and serial numbers, for example)	Ranges from work starting to DP	Undecided
	ISO SC21/WG5	Defining parameters to be managed for upper-layer protocols. For example, which system is to initiate sending	Ranges from work starting to DP	Undecided
	ISO SC6/WG2 & ISO SC21/WG4	Defining parameters to be managed for lower-layer protocols. For example, timers specifying retransmission timeouts and timers registering number of packets sent	WD	1991
	IEEE 802.2-802.10	Defining parameters to be managed for lower-layer protocols for LANs and metropolitan area NWs includes security	Ranges from beginning effort to DIS	Undecided
Managed Objects	ANSI ASC X3T9.5	Defining parameters to be managed for high-speed fiber-optic LANs	Work starting	Undecided
	ANSI ASC TlM1.5	Defining parameters to be managed for telecommunication devices such as multiplexers	WD	Undecided
	CCITT various SGs	Defining parameters to be used in communications such as those for ISDN	Work starting	Undecided
	IAB MIB WG	Defining parameters to be managed for the Internet's TCP/IP	RFC	Version 1 Complete

multi-vendor, multi-element, multi-domain networks. Network management products are offered by many equipment manufacturers, by third-party organizations, and by users who develop in-house products to meet their specific management needs when solutions are not available from off-the-shelf products.

As noted in Section 2, the capabilities for network management systems that users desire most are interoperability of products from different vendors and integration of the capabilities to manage a wide variety of individual components in a single system. The disappearance of user-perceived difficulties in performing end-to-end management of the network is sometimes described as a "seamless" view of the network. The management capabilities available in this seamless view of the network include the following:

- indication of operational status of the network and its elements
- collection of network performance information
- ability to track user activity and change network configurations
- collection of billing statistics
- ability to communicate with devices located throughout the network from a central or remote location
- a management interface to network elements that is consistent across multiple network elements and multiple vendors' products, where implementation is uniform and intuitive to use, that is, user-friendly.

The formal set of guidelines for describing the functionality of network management products that vendors are providing or toward which they are directing the development of their products, are guidelines set forth by the ISO in the development of Open Systems Interconnection (OSI) network management standards[22]. These standards and implementation guidelines deal with both the standardization of syntax (structure) and semantics (meaning) of information exchanged between heterogenous systems.

[22] As initially noted in Section 2.2 and discussed in detail in Appendix B, the framework for OSI Management is defined in Part 4 of the Basic Reference Model Standard (ISO/IEC, 1989). The OSI Network Management Forum, then, is following the ISO/IEC standards in developing specifications for network management implementations (OSI/Network Management Forum, 1990).

As discussed in Sections 2 and 3, the standardization of semantics resulted in the classification of management information into five functional areas: fault management, accounting management, configuration management, performance management, and security management. The information provided by these functional capabilities is used to satisfy four operational requirements: network operation, administration, maintenance, and planning and procurement.

Monitoring and reporting of service degradation (a part of the performance management function) and remote testing and restoration of network resources (a part of the fault management function) are widely regarded as among the most important aspects of network management. A recent survey[23] of 300 information systems managers from 1,000 large companies indicates the three most important features of network management to be security, performance tracking, and rerouting capability. The bar graph in Figure 26 shows summarized results from the survey.

4.1 Network Management Domains

Telecommunication networks that support voice, data, video, messaging technologies, etc., designed according to an organization's (or corporation's) priorities, have been termed Enterprise Networks. These enterprise-wide networks provide intrafacility services for the local organization and interfacility services for geographically separate organizations, encompassing operations that may utilize both public and private networks. It follows that management of these networks has been termed Enterprise Network Management (ENM). A management capability that provides ENM is integrated across all of the enterprise network domains.

Characteristics of voice network management are unique and different from those for data network management. Also unique is the management of transmission services that are common to both the voice and data networks. As interaction among services continues to increase, boundaries between transport, data, and voice services tend to become blurry at best. With continued higher level integration, the current voice, data, and transport domains are migrating toward logical rather than physical categories.

[23] Summarized results of the survey conducted by the Business Research Group, Newton, Massachusetts, were reported in the LOCAL NETWORKING Section of *NETWORK WORLD*, issue dated December 23, 1991.

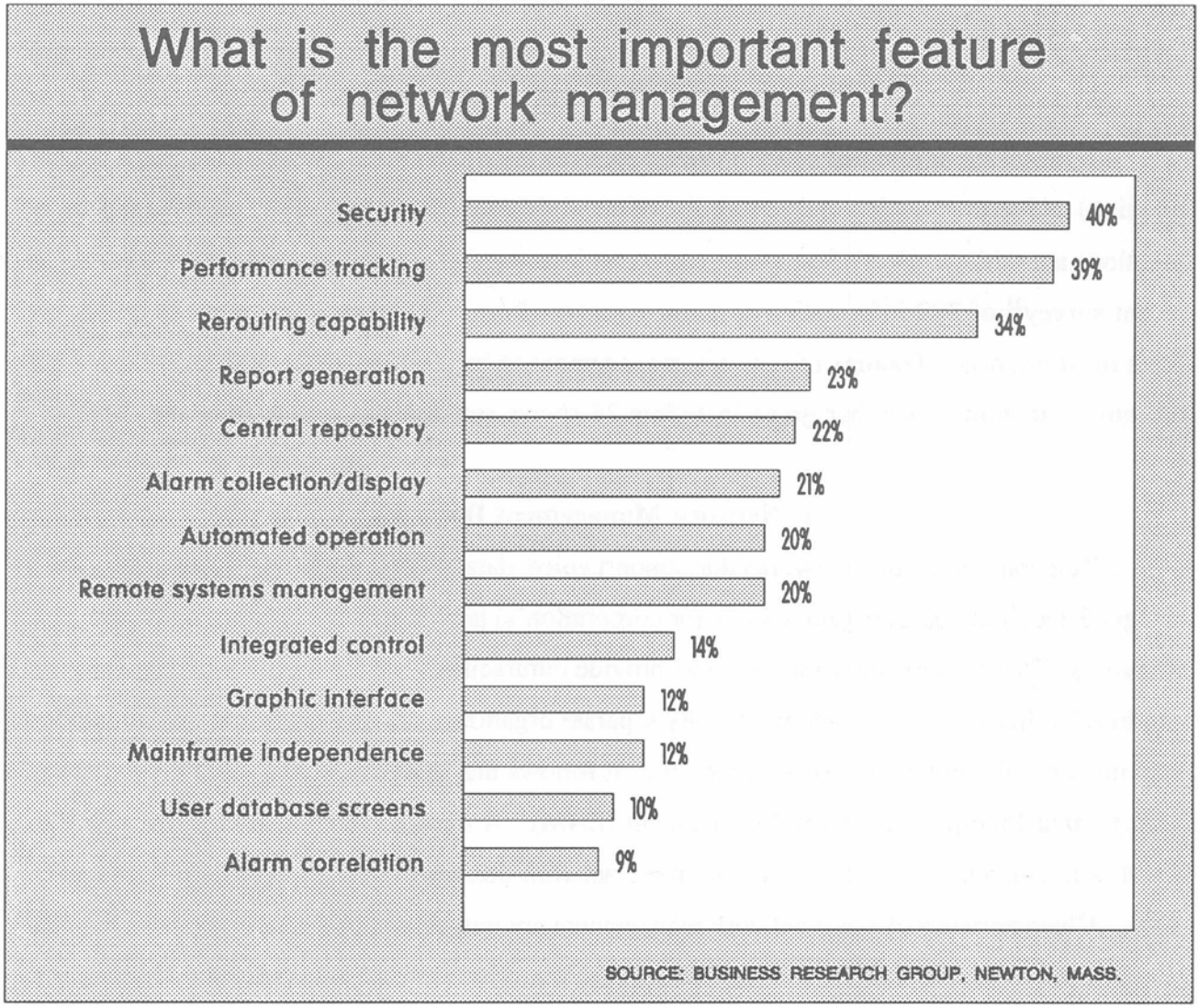


Figure 26. Results indicating most important features of network management (for local networking) (based on original graphic by Mitchell, 1991).

However, in order to describe the scope of today's network management products and their role in the management of the network, we have elected to identify three network management domains that parallel what seems to be a natural classification of the products themselves. The three domains, originally defined by Goldsmith and Vizcaino (1989) and depicted in Figure 27, are the Transport Management Domain, the Data Management Domain, and the Voice Management Domain.

- **Transport Management** is management of network resources that provide transmission of services without actual involvement in the service itself. Modems, multiplexers, bridges, packet switches, satellite systems, and microwave facilities are examples of these resources. These devices perform their functions without regard for the service being carried (e.g., voice, data, video).

- **Data Management** is concerned with management of network resources (elements) associated with data-communication end nodes. These elements include data-processing computers, front-end processors, terminal controllers, workstations, terminals, printers, local area networks, hubs, and concentrators.

- **Voice Management** provides management of network resources (elements) associated with the telephone system. Three major components of telephone networks are the station equipment, transmission facilities, and switching facilities. However, the transmission facilities are considered to be part of the Transport Management Domain. The remaining station equipment and switching facilities are comprised of elements that include PBXs, key systems, and electronic switching systems.

The classification of network management domains just described leaves open the question of network management for ISDN. There is good reason for this. CCITT Question 9/II (CCITT, 1988), concerning international network management, that is allocated to Study Group II for the 1989-1992 study period asks:

> "What new Recommendations, or changes to existing Recommendations, are necessary to provide guidance on the network management surveillance and control capabilities which may be necessary for the ISDN, and in particular during the transition to ISDN?"

Until guidance, or standards, for ISDN network management are available, or users "demand" the capability, ISDN management products will not be developed. That was essentially the state of the technology in 1992.

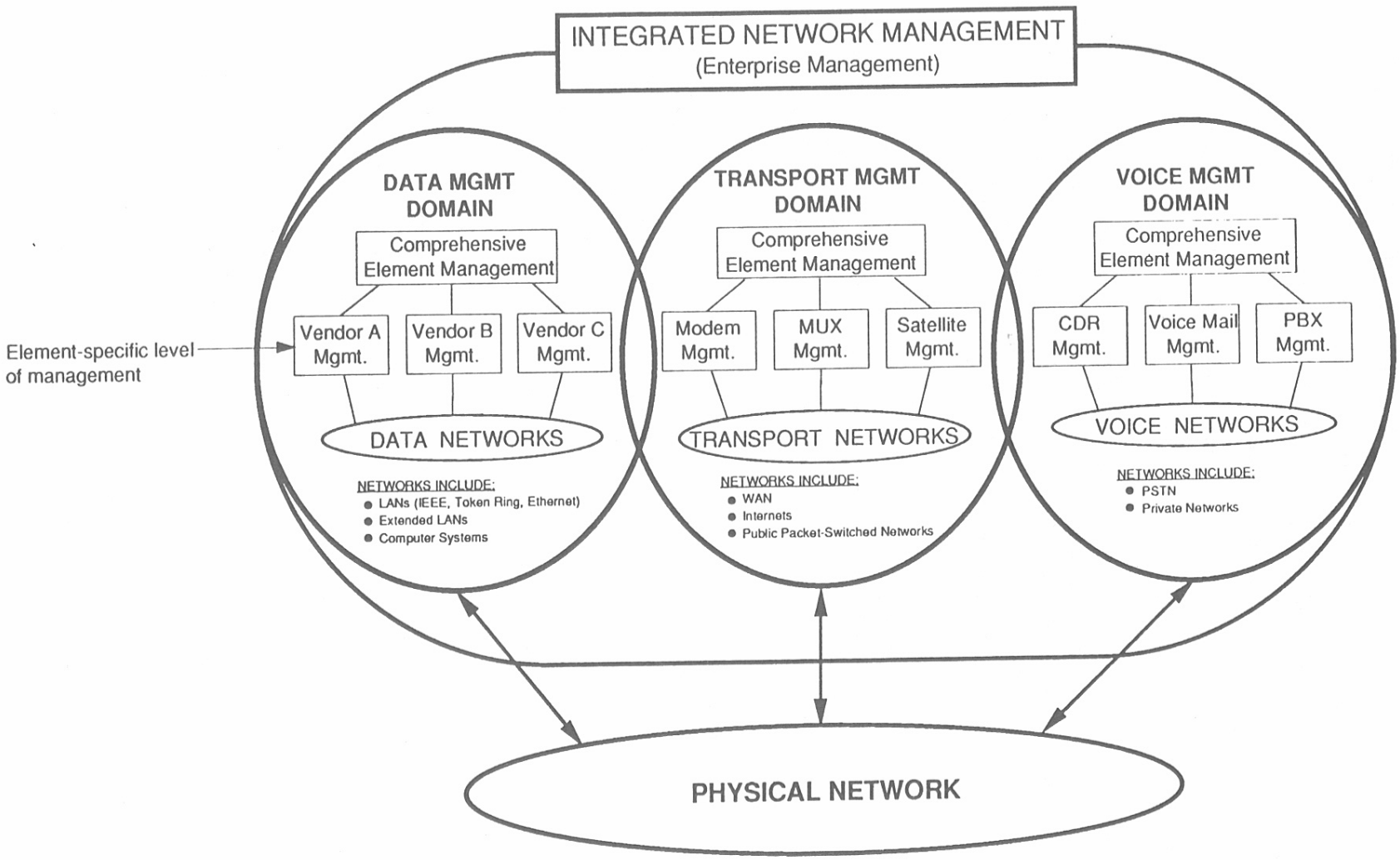


Figure 27. Network management domains showing hierarchical management architecture within each domain.

The trend of network management is to integrate management of services and elements across all domains. As noted earlier, integration across all three domains often is considered to be Integrated Network Management, also commonly referred to as Enterprise Network Management. Within each domain, management is further subdivided into Element-Specific Management and Comprehensive Element Management.

- **Element-Specific Management** is vendor oriented and usually encompassed as part of the network element. These products manage a single network element or more than one element of the same family and are tasked with surveillance and control of the network elements they support. Element management systems are autonomous network management systems serving to manage that specific portion or component of a network and generally do not manage all components of a network end-to-end.

- **Comprehensive Element Management** manages families of single-vendor elements as well as like elements of multiple vendors. Therefore, there may exist multiple element-specific and/or comprehensive element management in a single network.

The functionality of network management products is discussed in the remainder of Section 4 as it applies to specific domains. While management systems that interface with multiple vendors' products and systems are evolving, technology has not yet produced a single, consistent family of products to support an enterprise-wide, multi-vendor environment. Today's network management solutions make use of multiple tools to manage the heterogeneous network.

4.2 Products for Management Within the Transport Domain

The Transport Domain provides the end-to-end transmission of services. The networks of concern to the Transport Domain are those that interconnect networks found in both the Voice and Data Domains. Transport Domain elements include communications processors, communications switches, analog leased-line modems, digital leased-line channel service units, multiplexers or T1 nodal processors, packet switches, data switches, packet assembler/disassemblers (PADs), and gateways. The Datapro Reports[24] are among the sources

[24] Datapro Reports that were consulted during the preparation of this report include Reports on Telecommunications, Reports on Management of Telecommunications, Reports on Data Communications, Reports on Managing Data Networks, and Reports on Network Management Systems. These Reports are available from McGraw-Hill, Inc., Datapro Research Group, Delran, NJ 08075.

of information about network management products. Information from these reports has been used throughout this section of the report; individual authors are cited in the references.

The functional characteristics of management products for the Transport Domain include transmission performance monitoring, fault monitoring and isolation, and configuration management. These functions provide a network manager with physical information on the status of an element, its interface with the terminal equipment, its interface with the transmission facility, and the condition of the transmission facility.

4.2.1 Element-Specific Management Tools

Element management systems in the Transport Domain are characterized by their limitation in managing a single network element. A simple example of a Transport Domain element and its management is a modem and modem manager.

The type of modem found in a network varies depending on the application. Datapro has issued three reports on modem technology and the modem market (Callahan, 1991). Considering only those modems that provide low-, medium-, and high-speed data rates, over 640 modems are available from more than 90 vendors. Most of these modem products in use, however, seem to be offered by no more than 15 vendors. The Datapro Reports also list information for limited-distance modems, fiber-optics modems, line drivers, modem eliminators, and radio-frequency modems.

Modem management includes the capability to monitor modem status as well as connection status, perform diagnostics, and configure the modem. Monitoring includes the detection of connection faults and connection integrity, with access to diagnostic capabilities when problems are encountered. Configuration includes setting of line and port configurations, data rates, input device characteristics, terminal options, and time and date for event-logging. Diagnostic capabilities typically include the capability for local and/or remote loop-back testing for error rate measurements and trouble shooting.

In addition to the built-in configuration or setup command structure local to many modems and accessed through straps, thumb-wheels, or DIP (dual in-line package) switches, "intelligent" modems typically are configured through a computer keyboard. Vendors have developed software applications which provide the capability to manage the device through a management console or personal computer providing a more "user-friendly" interface. These

software applications, depending on their sophistication, provide the capability to manage single or multiple modems of the same vendor as well as multi-vendor modem products. Such applications may be a module of the overall, network management capability. Some typical examples of modem management products, generally incorporating the features that have been discussed, include the OSI 821 from Octocom Systems, Incorporated; the High Density Management System (HDMS) from Microcom, Incorporated; and the Modem Management System from Digilog, Incorporated.

4.2.2 Comprehensive Element Management

A common and attainable vendor objective is to integrate network management among different elements from a single vendor's product line or across multiple vendors' products for the same functionality. These types of systems integrate management of the vendor's network components such as modems, multiplexers, data service units (DSUs), and switching equipment within any domain. Comprehensive management systems monitor multiple network components to provide early detection and isolation of failures, perform diagnostic tests, record configuration and performance information, display that information, maintain databases on inventory and history, and generate reports for management based on the information in databases. This is much the same functionality as is available in many element-specific management systems, but the comprehensive management systems offer a network-wide view of all the elements accessible from a single vendor. Examples of such systems include AT&T Paradyne's Comsphere[25] 6820 Network Management System, the Network Analysis and Management System (NAMS) from Digilog, Incorporated; the Network Control and Management System/Personal Computer 386 (NCMS/PC 386) from NEC America, Incorporated; and the Network Management Control System (NMCS) — 2500 Rise 1 from Tellabs, Incorporated. Each of these systems is used for managing that vendor's product line of modems.

These types of products are configurable or available as entry-level, mid-range, and full-feature products, respective of the number and type of network elements to be managed and

[25] Comsphere is an AT&T Paradyne product name, established after AT&T's acquisition of Paradyne Corporation in 1989, for Element Management Systems that supersede both the AT&T Dataphone II System Controller NMS and the Paradyne Analysis NMS.

features and functionality offered by the product. Some of the enhanced features include the following:

- capability to monitor a larger number of network elements
- capability to offer more-powerful hardware platforms and, additionally, local and remote network consoles
- capability to interface to other high-end and low-end integrated management packages
- capability to provide extensive report generation
- capabilities for enhanced diagnosis and testing.

Management products are available for managing families of CSUs, multiplexers, and many more elements. Obviously, the functionality available in the management system will depend on the functionality incorporated into the network elements. Figure 28 depicts AT&T Paradyne's Comsphere 6820 Network Management System which is representative of the types of hardware and software features that these systems typically provide.

4.3 Products for Management Within the Data Domain

Products within the Data Domain manage those resources usually associated with the end nodes of data communication networks. These data networks typically are established as logical networks that are end-to-end and virtual-circuit oriented. An application residing on one of the network entities establishes and carries-on a session with a user or other application without regard for the transport components.

The elements to be managed in the Data Domain are components associated with data networks. These elements include terminal controllers, hubs, terminal servers, file servers, bridges, routers, computer systems, and single or multiple (extended) LANs. The network within the Data Domain is characterized by its inherent local operation, user ownership, limited geographical coverage (usually within a facility, encompassing multiple floors and rooms), high-speed (large-bandwidth), and virtual-switching technology.

Figure 29 depicts the relationship of management tool complexity as a function of network complexity. As the data network grows from simple PC networks to interconnected

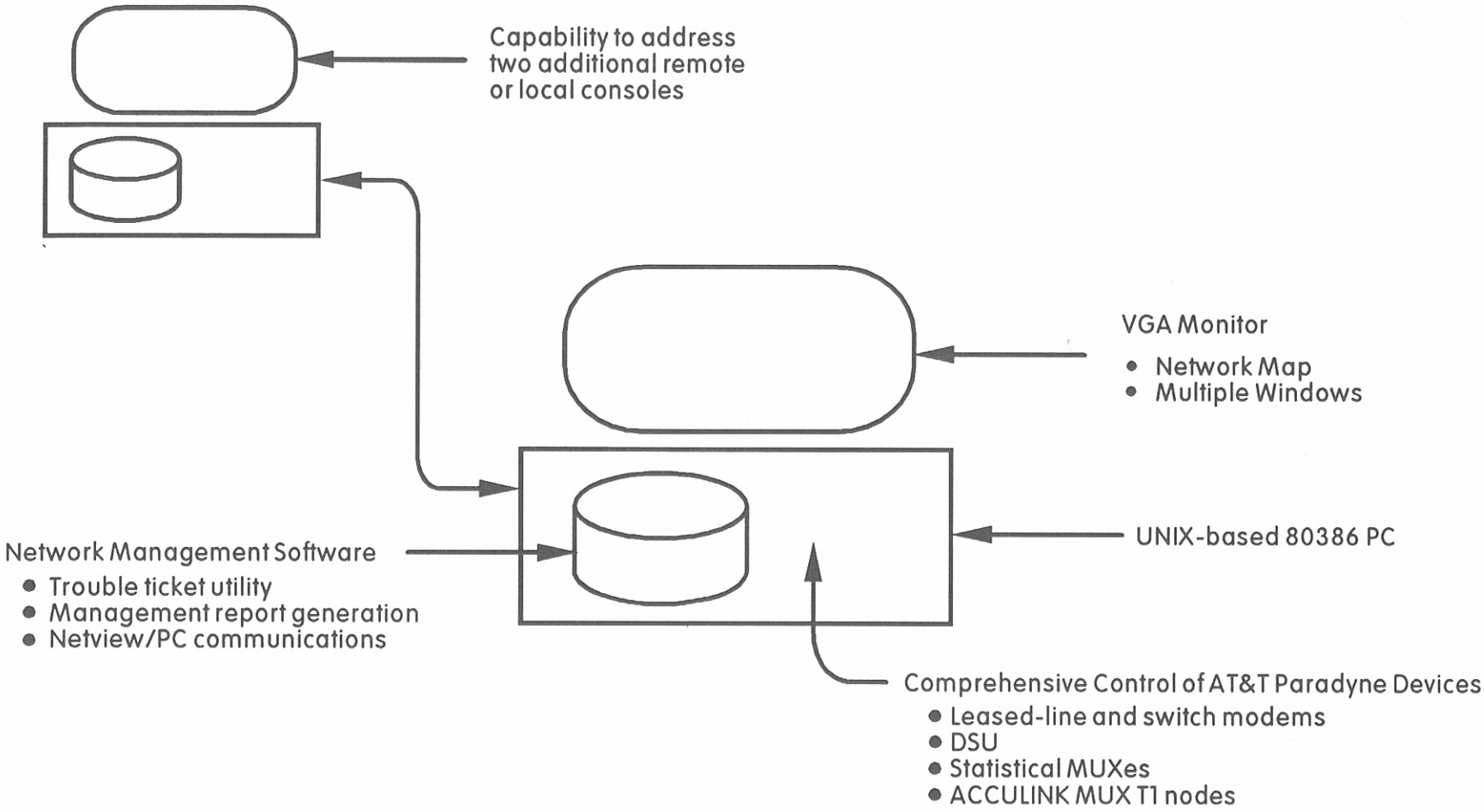


Figure 28. Example of a comprehensive network management system--AT&T Paradyne Comsphere 6820 Network Management System.

networks and into extended networks, the tools required to manage the network tend to be more encompassing and complex. The tools are used for diagnosis of hardware malfunctions and cable related problems, software and network configuration related troubles, or a combination of these. The choice of tools to use is influenced by the size, complexity, and criticality of the network. Examples of hardware diagnostic tools for testing and analyzing data networks include protocol analyzers; tools for detailed signal measurement and observation, such as oscilloscopes; and tools for fault locating, such as time-domain reflectometers. Tools that are useful in solving network or software related problems include the capabilities available in network operating systems (NOSs). The NOS also serves to configure and administer the network, alert the user of potential performance or security problems, and much more. Many of the software tools initially available as add-on tools to the NOS now are being built into the NOS, thus allowing more comprehensive management from the NOS.

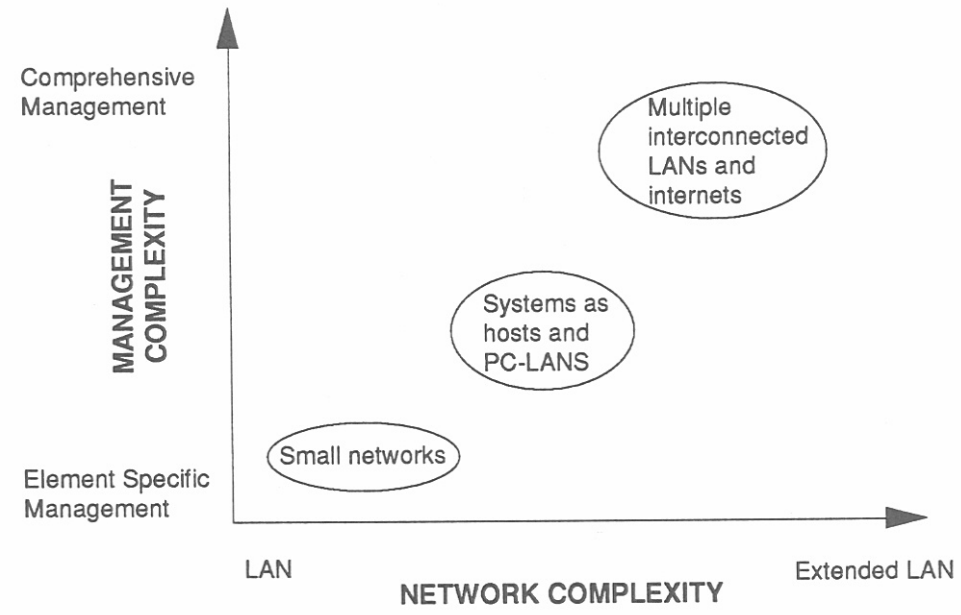


Figure 29. Management complexity as a function of network complexity.

The problem encountered today is that each of the interconnected networks has its own management system and each of the elements on each network has its own management system. According to Caruso (1990), as noted in Section 2, the highest-priority needs today in network management are the ability for products from different vendors to interoperate and the ability to

manage a wide variety of network elements with a single system. Unfortunately, such capabilities are not yet available. Management of multi-vendor devices, hence multi-vendor management systems, requires management standards. Until such standards are available, many vendors have designed for uniform management across their own product lines.

The functionality associated with data network management products is much the same as that required for managing the Transport Domain networks. Such functionality includes the capability to obtain and analyze element and network performance statistics; locate, correct, and record element and network fault conditions; configure and administer the network; and maintain and bill for services and network use. Table 9 lists the functionality available in data network management products. The functional features are described according to the ISO-defined management categories (ISO/IEC, 1989), with the addition of User Administration to emphasize the day-to-day user involvement in a variety of tasks concerned with adjustments to configuration of the network.

Table 9. Typical LAN Management Functionality

Management Category	Typical Management Functions
Fault	Fault detection, isolation and correction; system restoral; help desk
Accounting	Billing and chargeback, usage statistics, software compliance
Configuration	Network inventory, device configuration, directory management, disk management
Performance	Traffic statistics and analysis, network availability, diagnostic testing
Security	Password administration, access rights, backup and disaster recovery, security audit trail
User Administration	User support and training

4.3.1 Element-Specific Management Tools

At the element-specific level of management, the functionality required of Data Domain management systems typically is limited to performance, fault, and configuration. Dedicated measurement devices provide fault locating and performance functionality through monitoring and testing of network elements, with possible additional functionality for diagnostic testing, restoral, and obtaining network transmission statistics. Typical examples of these devices include LAN (or protocol) analyzers, network monitoring and recording devices, and time-domain reflectometers.

LAN analyzers are used to aid in trouble-shooting local area networks. They allow analysis of data packets on the LAN, examination of node interactions, and monitoring of network traffic. These functions provide insight into network throughput and help in identifying bottlenecks. Information about LAN traffic patterns can help solve hardware-related problems, such as slow response time for a particular user or congested traffic across the network. Network analyzers are available from several manufacturers and each offers a unique complement of features. Typical features would include menu-driven feature selections, function-key control, data-frame filtering, start/stop data-frame triggers, capture-buffer data/frame search, and frame time-stamping. Although these features are common, their implementation and degree of functionality across vendors' products distinguish one product from another. Among the many LAN analyzers available, typical examples include Network General Corporation's LAN protocol analyzer called Sniffer, Excelan's (the Products Division for Novell, Incorporated) LANalyzer, and HP's 4972A LAN Analyzer for IEEE 802.3 LANs.

The typical functionality offered by monitoring devices includes collecting traffic statistics and monitoring network usage. Examples of products include DEC's LAN Traffic Monitor, the ARCnet Analyzer (ARCAN) from Anasys, Incorporated for monitoring ARCnet networks, and TRW's LanStat packet monitor for analyzing the performance of Ethernet devices.

In addition to the hardware versions of these tools, software complements are available. The software versions may provide more limited capability as well as some features not available from their hardware counterparts. Examples include Brightwork's LAN diagnostic software, E-Monitor for Ethernet networks and ARCMonitor for ARCnets, LANtool's LANtraffic, and Farrallon's TrafficWatch.

There are a host of other similar products which offer the same functionality as the products listed here. These software tools allow the manager to attempt to quickly and conveniently diagnose and locate problems without involving the setup of the hardware tools. Dozens of these type products are available with much the same functionality. But, the point of emphasis is that these analysis and monitoring products are designed to perform limited functions, namely performance and fault isolation, and are designed to work for specific network architectures.

4.3.2 Comprehensive Element Management

Comprehensive element management in the data domain typically is provided either as embedded functionality in the network operating system for small network environments or as separate functionality for multiple-segment LANs and internet environments.

The Network Operating System as a Tool in Network Management

The network operating system manages the interface between the network's underlying transport capabilities and the applications resident on network servers (Marney-Petix, 1992). Examples of network operating system products include Novell's Netware, Banyan's Vines, Microsoft's Lan Manager, AT&T's LAN Manager/X, and Ungermann-Bass' Net/One. Network operating system vendors embed limited network management utilities within the network itself. Table 10 lists management functionality that typically is embedded in network operating systems.

The typical function associated with a network operating system is that of managing the network server. This includes monitoring and allocating disc storage space, server access, network application access, and configuration. The network operating system also offers network-wide services such as configuring network devices, monitoring on-line system usage, detecting failed stations, and rebooting network devices.

The hardware platform on which a network operating system runs may be a PC, a workstation, or a mainframe computer. The operating system may be DOS, IBM's OS/2, a Macintosh operating system, or UNIX software, as appropriate. The station then serves as the network or system console from which the network is controlled and administered. Some of the vendors of network operating system products allow limited administration of the network from

remote terminals. In addition to the system console, each station on the LAN typically requires a LAN adapter card that can interoperate with the network operating system.

Table 10. Typical Network Operating System Management Functionality

Management Category	Typical Embedded Management Functions
Fault	Fault detection, problem reporting, communications link diagnosis
Accounting	Usage statistics
Configuration	Device configuration, backup control, LAN device administration, mirroring, central administration
Performance	Traffic analysis and statistics, server CPU usage, performance alerts, disk usage
Security	Password administration, access privileges, backup and disaster recovery, security alerts, audit trails

In addition to the capabilities built into the network operating system, third-party utilities (i.e., software applications) have emerged that augment the LAN network operating system by adding or enhancing network operating system functionality. These utilities or applications fill a niche by providing additional features or functionality that are not available from the network operating system vendor. Some examples include collecting and displaying file server statistics, implementing a help desk, and problem-tracking services, file locating utilities, remote user utilities, and menu generating and customizing utilities.

Multi-segment and Internetwork Management

As the network expands, it becomes necessary to manage multiple elements and multiple LAN segments, such as for campus and internet environments. In most cases the management of internet or campus-wide networks is dependant on the overall network architecture. The more diverse the segments, the less likely it is that a multi-segment network can be managed as an

integrated unit. Various products offer the capability to manage groups of elements of interconnected LANs or network segments. These products are characterized by their capability to perform centralized and/or remote monitoring of multi-segment LANs or internetworks. These products communicate with multiple network elements including bridges, PCs/hosts, FDDI rings, routers, and hubs. They communicate through a variety of network management protocols including the SNMP, the Common Management Information Protocol, the CMIP Over TCP (CMOT), the CMIP Over Logic Link Control (LLC) (CMOL), DECnet's proprietary Network Information Control Exchange (NICE), IBM's proprietary Network Management Vector Transport (NMVT), and more. They also provide capabilities to interface and support "integrated" network management systems, including AT&T ACCUMASTER Integrator, DEC's Enterprise Management Architecture (EMA), HP OpenView, IBM NetView and others.

A typical comprehensive management system runs on a PC or workstation platform using local and remote software. The remote software, often called an agent, resides in the device being managed. A popular management platform is the Sun SPARCstation for supporting the increasingly sophisticated graphical user interfaces used to portray network topology. UNIX also is popular as the operating system of choice for these management systems due to its multi-tasking capabilities and its openness. The functional characteristics offered by these systems usually are more enhanced and the features offered are more extensive than for the element-specific management systems, due to the complexity and variety of elements with which these management systems must interface and communicate (Datapro, 1991).

Under fault management, the comprehensive management systems alert the operator to a failure or degrading condition by using a scheme of alarms. When a local or remote monitor detects a problem it activates an alarm at the operator station. Management systems typically provide a positive alarm signal, an audible sound and/or a console message, noting the type of element malfunctioning, the location, and the nature of the failure.

Accounting management is supported by charge-back utilities that tally up usage by user, application, or other criteria. Usage may be counted in packets sent, packets received, time spent on the network, or any number of metrics.

Configuration management support usually takes the form of a graphical map depicting network topology, plus an inventory database with information on attached network devices. Many systems allow an operator to bring-up an inventory record just by selecting an icon that

represents a particular device on the network map. The inventory record may include network address, network type, and identification information along with a contact name and phone number for reporting problems. Some management systems support auto-topology which is the capability to automatically create a network map by polling all attached network nodes and examining the destination/source address of each frame. Map-editing tools are necessary to create a final network picture which makes sense to the user, grouping network devices according to geographical, functional, or organizational boundaries.

Under performance management, most comprehensive management systems are capable of collecting traffic statistics such as bytes in/out, packets in/out, and errors in/out. The data are displayed in the form of bar graphs or strip charts for later analysis. More sophisticated systems support trend analysis applications and databases that allow the user to retrieve the information for later processing. Security management may encompass multi-level access and data encryption as well as support of a security audit trail feature.

The more comprehensive network management systems are available as turn-key systems from LAN vendors, such as 3COM Corporation and Ungermann-Bass, as well as systems vendors like HP, IBM, and Sun Microsystems, Incorporated. Examples of products from LAN vendors include 3COM Corporation's Network Control Server and Ungermann-Bass' NetDirector. Examples of comprehensive management products from systems vendors include HP's OpenView Network Node Manager, IBM's LAN Network Manager, and Sun Microsystems', Incorporated SunNet Manager. Others include AT&T's Systems Manager, Northern Telecom's DPN (Data Packet Network) LANscope Remote and, Cabletron Systems', Incorporated LANVIEW/SunNet Manager and also their Spectrum product. These vendors typically ensure the interoperation of their proprietary network management products with their own network operating system. They may not integrate with other LAN vendors' network operating systems or network management architectures. Many of the network operating system vendors have linkages to standard and popular, proprietary management architectures via SNMP or other network management protocols.

Each network operating system can serve network management needs for a certain optimal network size and complexity. For the operating system to play its role within the overall internet architecture, it must operate as part of the overall network management architecture. Therefore, the monitoring and control that the network operating system performs must include pass-through

and reporting of significant events and status to the management information base of the overall network management architecture (Marney-Petix, 1992).

4.4 Products for Management in the Voice Domain

As stated earlier, the two components of the telephone network within the Voice Domain are the station equipment and the switching facilities. The third component, the transmission facilities, is considered part of the Transport Domain. Voice Domain network elements include PBX, voice messaging (mail) systems, automated call distribution systems, and call detail recording (CDR) systems. Management of voice networks (sometimes termed telemanagement) may utilize in-house staff, contracted facilities management services, and carrier provided management services. The focus of this section of the report is on products for management of network elements. There is only brief mention of management services offered by third party organizations or the local and long-haul carriers.

Typically, the management system for Voice Domain network elements is proprietary, designed for the specific system, and supplied by the vendor who supplies the equipment with separate system consoles to interface to each element. From a products prospective, network management of voice networks is subtly different from management of data networks. At both the element-specific level and comprehensive-element level of management, the emphasis of products is on management of the features and functionality offered from the network with less emphasis on the network itself. Management of the network has evolved to be well-defined and well-understood. Voice Domain networks typically are not as diverse as data networks. They require a relatively limited number and variety of elements to achieve a fully functional voice network.

4.4.1 Element-Specific Management

At the element-specific level of management, each element is managed through the management system inherent to that element. For example, voice mail systems, automated call distribution systems, and PBXs each require separate interfaces and management systems.

Furthermore, basic capabilities for identifying and monitoring network performance conditions, such as basic alarms and line errors, are integral to diagnostic software residing in today's digital PBXs. PBX and key system manufacturers have developed software that allows

a network administrator to be able to monitor line status. PBX-resident diagnostic programs provide a limited database from which outage reports can be generated on an administrative printer terminal. Some PBXs offer automated centers with voice-mail or message-recording capabilities. Directory systems are another popular enhancement being integrated into some PBX systems. At an attendant's station, it is highly desirable for the operator to be able to key in the first few letters of the called person's name to get a screen-full of names and station numbers. Another popular enhancement for PBXs is inventory management systems. These are multi-functional, PC-based systems that support line inventories, equipment inventories, trouble reporting, and service reporting. Many systems now provide the capability to monitor and manage network performance problems automatically from a central location (Llana, 1990).

4.4.2 Comprehensive Element Management

The trend is integration of Voice Domain network elements by integrating the functions of separate elements into the PBX. As an example, PBXs now are offering built-in voice messaging, automatic call distribution (ACD) capabilities, and call detail recording services. Such PBXs have the same features available from separate elements and other enhanced features not offered by the separate elements.

These telephone management systems (TMSs) offer a wider variety of functions some of which include report generation and help in optimizing network facilities and maintaining work orders, equipment inventory, cable management, and directory databases. TMS products range from turn-key, stand-alone systems to software packages that run on microcomputers, minicomputers, and mainframe computers. Many users turn to the vendor who supplies their telephone systems for TMS support. Vendors who specialize in TMS tend to emphasize their own functionality and ease of use as superior. Service bureaus have traditionally had a significant influence. Computer-based TMS that are corporately installed and controlled, with reports and functions designed and delivered to suit corporate agendas, have become increasingly popular, replacing other options. Microcomputer-based systems account for an increasing share of the market, echoing a trend in computing in general. The results of a Datapro survey, taken in February 1990, revealed a considerable mix of products. Vendors are not restricted to a single hardware platform. Many offer a mix of systems that includes turn-key as well as

software-based. This allows them to meet a variety of TMS needs for small and large customers (Womack, 1990).

The movement toward software packages that include more integrated functions and provide assistance in analyzing present and future needs is one of the major trends in this market. Users are demanding the ability to add functions as needed without expensive upgrades or replacements. Another trend is modular software design which allows this movement to occur smoothly. The user purchases only the software that is required at a specific time and adds on as needed.

Vendors are offering more features, more efficient migration and integration, and more application-interface functions. Features that were once add-ons are integral to the system; integration is becoming "seamless," and applications interfaces are using the computer in conjunction with the PBX. Making "add-ons" standard features is one way for PBX vendors to capture market share. Call-detail recording, which now requires maintenance of a separate database, is an example. Integration into the PBX software will reduce maintenance time. Another potential area of improvement is voice mail. Stand-alone, voice-mail systems require not only trunk cards in both the PBX and the voice-mail processor, but they must also tie up a trunk to connect the two. "Seamless integration" and "smooth migration" are now common terms in PBX marketing. Vendors are responding to users' demands for systems allowing migration from old to new or small to large with minimal loss of initial investment. The users also want seamless integration to allow networked PBXs to appear as a single system to the user (Ricci, 1991).

Telephone management software systems evolved from relatively simple call accounting systems to complex systems supporting such critical operations management functions as traffic engineering, network design and optimization, inventory management, and work order and problem management. The effective performance of these functions serves not only to control costs and improve responsiveness to end users, but also to enhance the availability and general performance of the network itself. Low-end systems may provide only limited, call-accounting capability via software systems that reside on single-user PCs, and that support a single telephone system. High-end systems may satisfy a full range of functional requirements and run on mainframe computers that support hundreds of users and manage many geographically-dispersed telecommunication systems and other network resources. Additional variations include systems

that are designed to run on LANs and minicomputers. Telephone management systems may be proprietary — designed by a manufacturer to support a given telephone system — or switch independent (Goleniewski and Horak, 1991).

4.4.3 Functional Requirements

Telephone management systems address a wide range of functional requirements and provide capabilities to satisfy those requirements in several ways. Many low-end systems are limited to call accounting, which may be based on estimates of numbers of calls. High-end systems address a much broader range of responsibilities and provide more depth of functionality. Such functionality typically is delivered on a modular basis, with all modules relying on a single, synchronized, management-information database. Traditional telephone management functions include

- call accounting and management
- call allocation and management
- asset management
  - inventory management
  - cable and wire management
- process management
  - traffic analysis and engineering
  - network design and optimization
  - directory management
  - work order/service order management
  - trouble/problem management.

Bill recognition, contract and vendor management, circuit management, data-connectivity tracking, ACD management, project- and personnel-scheduling management, and physical network management functions also are available in some telephone management systems (Goleniewski and Horak, 1991).

Computing Environment

Contemporary telephone management software systems originally were designed to operate in a specific host computing environment, e.g., mainframe, minicomputer, or personal

computer. Relatively few, fully-functional, mainframe-based systems currently are marketed on an active basis, but most of those marketed are designed for IBM or IBM-compatible environments. Examples of developers and suppliers who provide these tailored products are Cincinnati Bell Information Systems (CBIS), Stonehouse & Company, Telco Research Corporation, and Westinghouse Communications.

Minicomputer-based systems typically have their origins in custom programming efforts for large clients with multi-user requirements. These systems are largely designed for either DEC or AT&T UNIX computers. Few vendors compete in this market segment, but those who do offer systems with a relatively broad range of functionality. Examples of organizations who develop and market these products are AT&T, ComSoft Management Systems, The Info Group, Stonehouse & Company, Telecommunications Software Inc., and Telco Research Corporation.

PC-based systems represent by far the most competitive market segment. The vast majority of telephone software systems are PC-based. Most PC systems are low in functionality and feature content, as they are single-user systems and intended for large-scale distribution. A few have substantial functionality and feature content, though they generally do not match the performance of mainframe and minicomputer-based systems.

LAN-based telephone management systems have appeared only recently and are few in number. The lack of LAN management standards, coupled with the fact that the LAN environment generally is very poorly controlled, has caused most vendors to avoid this platform. Telecommunications Software Inc. and XTEND Communications are examples of developers and suppliers of LAN-based telephone management systems (Goleniewski and Horak, 1991).

As the Voice and Data Domains continue to merge, the differences between telemanagement and other network management software systems will blur. A number of computer manufacturers are incorporating telemanagement functionality into the management systems traditionally used to manage data networks; IBM's NetView is an example. Furthermore, a number of telemanagement software vendors are incorporating into their products limited network management capabilities that generally are voice-oriented and designed to provide PBX management interfaces. AT&T, The Info Group, and XTEND Communications have all developed or acquired such capabilities.

The increased requirement for meaningful interfaces between telemanagement and other network management software systems raises the issues of database architecture and the interface

standards. Database architecture addresses the fact that network management software systems rely heavily on a MIB, which is the repository for all information describing the network characteristics, sub-networks, and the network elements (components). Many manufacturers of network management software systems have defined standard interfaces to other systems; AT&T Unified Network Management Architecture (UNMA) and IBM NetView are examples.

Standards also affect network management in terms of exchanging information between the network components and the various software management systems. Familiar protocol standards include many that are compliant with the OSI model. Manufacturers of voice communications systems generally have embraced this standard; data equipment vendors are less enthusiastic, as they have invested heavily in the development and support of proprietary standards, such as SNMP for TCP/IP environments and the NetView products for IBM's SNA environments. This investment is particularly evident in the LAN market

While network management standards currently are not a significant issue in telemanagement systems, these standards will be required to address the administrative aspects of network management. Therefore, telemanagement vendors will be required to understand the associated standards-based issues and become involved in the standards-making processes (Goleniewski and Horak, 1991).

Carrier-Provided Network Management Services

Increasingly, the local- and inter-exchange carriers are offering management services to support users' requirements for network management. Examples are the services called Insight, offered by US Sprint, and Integrated Network Management Service (INMS), offered by Microwave Communications, Incorporated (MCI). Functionality varies according to each carrier and may include statistical reporting, trouble-ticket reporting, line-error reporting, various levels of alarm reporting, and performance reporting that includes service outages and threshold alarms, such as frame slips and out-of-frame conditions (Llana, 1990).

In addition to the carriers, there are numerous other third-party organizations in the business of providing network management services. Considering the emphasis that users place on achieving very high availability of their networks and the technical complexity and specialized skills that are required to realize this objective, along with the growing difficulty that many

organizations experience in finding qualified people, third-party network management services may be the answer.

A service known as Spectrum was developed several years ago by Pacific Telesis using a VAX-based network monitoring and control system. Spectrum later was sold to IBM where it was converted to NetView, with management services for multi-vendor networks being offered from IBM's Network Support Center. An integrated management capability has been developed and service is offered by International Telemanagement, based in Washington, DC, using Avant-Garde's Net Command as the integration platform. The network management services available from Electronic Data Systems, using their Information Management Center in Plano, Texas, are another example.

Before deciding to use third-party network management services, an organization must be confident that services purchased will be better than the organization could provide for itself. These third-party network managers must deal with the same limitations as others in standards and products offered by vendors in developing their network management capabilities. It, therefore, follows that these management service providers must demonstrate that their employees are highly skilled and that the business is well-organized and using state-of-the-art technology.

4.5 Products Addressing Integrated Network Management

Integrated network management, as depicted in Figure 27, implies management within and across the Data, Transport, and Voice Domains. Section 2 discussed some of the conceptual approaches and architectures that are suitable for managing multiple elements, multiple vendors, and multiple domains. These include the centralized, the distributed, and the hierarchical approaches, as well as various combinations of these approaches. Some of the products available today for integrated network management provide the capability to manage across domains as well as to manage networks, equipment and applications within single domains. This section introduces some of these products for management of the multi-element, multi-vendor, multi-domain networks, commonly referred to as enterprise-wide network management products or umbrella management products.

It is desirable to view the entire network from end-to-end through a single interface for monitoring and controlling components, systems, or sub-networks. Currently, there are no network management capabilities that offer an end-to-end view of a network across all three

domains. Some products offer limited management of multiple components from the same vendor operating in the same or multiple domains. Other products will provide limited management for multiple components from various vendors operating in a single domain. Most of these products, however, are limited to monitoring and alerting the user to potential or real trouble and do not provide control and configuration capabilities necessary to fix the trouble. Today, fixing the trouble requires the use of vendor-specific, management systems for the particular equipment, sub-network, or system experiencing trouble. Products that offer full feature monitoring and control are not yet available due to several factors, which include the lack of management standards, the lack of user applications necessary to interface with the particular element or element management system, and economics.

While the detailed functionality of integrated management systems is unique to each vendor's products, the functional areas where commonality does exist among products includes fault, configuration, performance, and security management. Today, functionality is limited to passive monitoring and network-information gathering without any capability to modify or reconfigure network elements. For interactive configuration and diagnostic testing of network elements, users must rely on the vendor-specific, element management system. Complexity of the overall network requires unique and enhanced features for integrated management systems. For example, fault management now includes alarm correlation, i.e., the comparison of multiple alarms to determine the most likely cause of an alarm and suppress any secondary alarms linked to the same problem.

Performance management includes the collection of statistics and generation of summaries that may be used by the network manager in planning and implementing networks and that include activity summaries, error counts, network traffic loading, systems resource utilization, and trunk and node utilization. Configuration management features include network mapping with automatic, real-time, element recognition; color-coded alarms; and a windows-based, graphical, user interface. Security management addresses access control such as establishing password protection levels and security audit trails.

The information collected and utilized by an integrated management system is stored and maintained in a network database. This information includes event and error statistics, element and network configuration information, network performance statistics, network history information, and security information for all managed objects in the network.

Integrated network management systems often must subscribe to proprietary architectures and de facto standards, as well as the more widely-utilized, IAB and ISO standards. In most cases where proprietary architectures and de facto standards are implemented, the vendors have defined a migration strategy in support of open systems and IAB and/or ISO standards. Products supporting the IAB-developed management standards include SNMP-based systems, although implementations of the SNMP protocol may differ between some vendors. Many products recognize the ISO/OSI communications infrastructure standards by supporting the CMIP and CMOT management protocols. Each of the vendors shown in Figure 30 has a migration strategy in support of the ISO/OSI standards. Support of ISO network management standards may vary among vendors, depending upon the migration strategy followed and their selection of ISO/OSI standards and services to be implemented in their products. AT&T for example, has defined an open architecture based on CCITT/ISO standards and implementation according to the OSI/NM Forum specifications.

From a products point of view, there are three dominant approaches used in the development of integrated management products. The first approach to achieving vendor-independent network management is through a management framework or platform upon which a network management solution can be built and tailored to the network. Integration in this approach covers management of multiple vendors' equipment utilized in providing particular services, without restriction to use of a particular architecture. Examples of such platforms include HP's OpenView Network Management Server and Sun Microsystem's SunNet Manager. OpenView is designed to integrate, at the data level, all systems and network management capabilities across all devices in the network. The HP OpenView architecture follows the OSI/NM Forum Management Framework. It also is designed to support implementations of the SNMP and the Common Management Information Protocol over TCP/IP for TCP/IP networks (Hewlett-Packard Company, 1989).

The platform approach centers on the development of management applications built upon an open architecture platform offering interface capabilities and development tools. The platform vendors rely on users, systems integrators, and software developers to provide the applications necessary to interface to a particular vendors' network elements and management systems. For example, HP's OpenView NM Server serves as the open-application, development environment

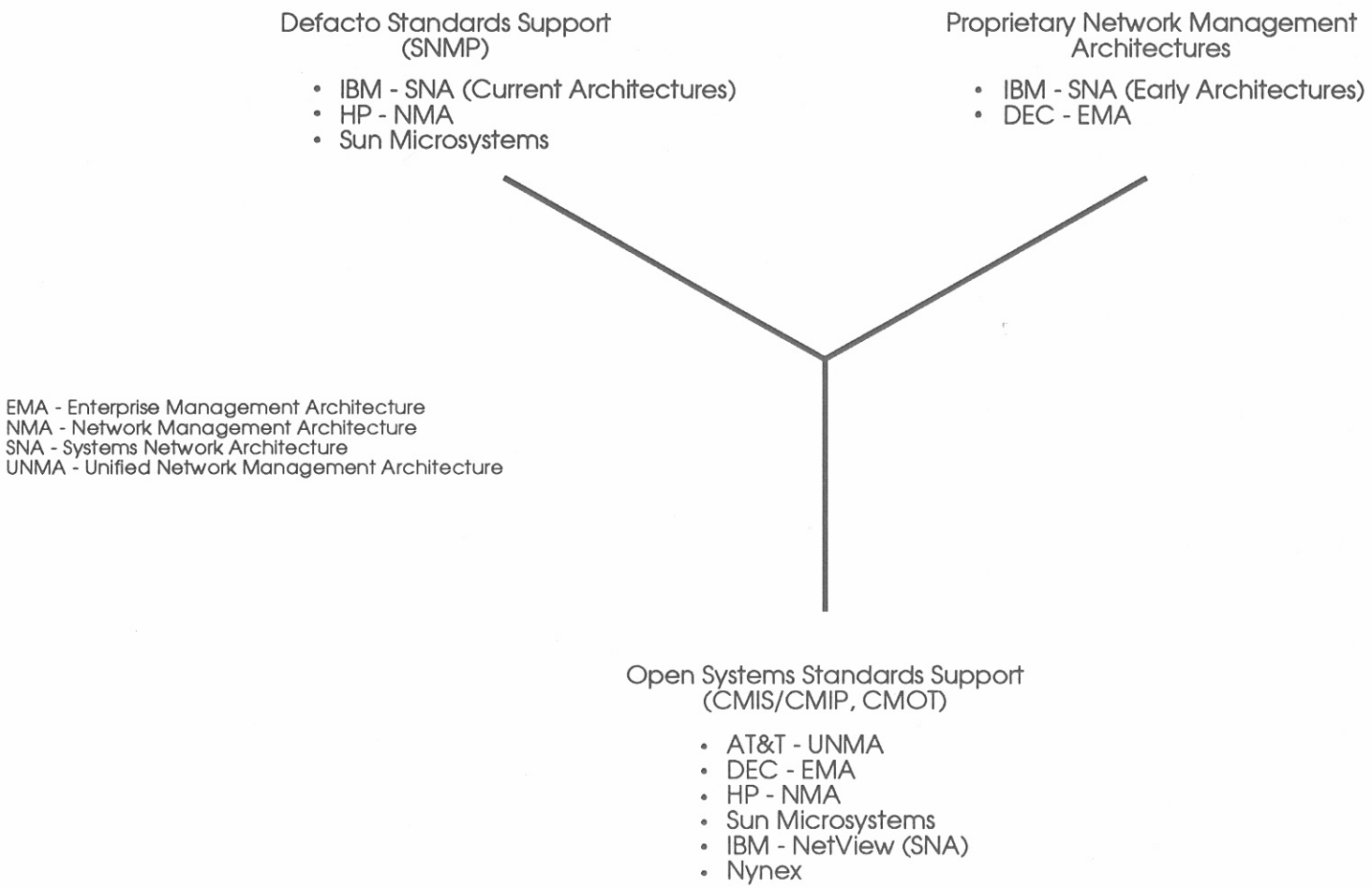


Figure 30. Examples of various vendors' support to network management standards.

for element- and integrated-management solutions based on HP's OpenView network management architecture.

The platform, application-development environments are used by software developers, systems integrators, and users to develop custom, network-management applications and to integrate network management applications from a variety of vendors. Synoptics, for example, has developed network management systems based on both HP's and Sun Microsystem's platforms. The resulting management system is marketed with each platform vendors' product lines (Jander, 1991).

The second approach is the development of products designed around proprietary system architectures such as IBM's SNA and DEC's DECNet architecture. Integration in this approach covers management of multi-vendor equipment used in providing particular services while conforming to a particular architecture. Management may be within a single domain or across any two or all three of the management domains. Both IBM and DEC have developed strategies for long-term, network-management integration. An example is DEC's Enterprise Management Architecture for enterprise management. Under the EMA architecture, the DECmcc Management Station consolidates DEC's existing management products into a single platform to provide users with a transition path from current DEC network management support to fully EMA-compliant enterprise network management (Axner, 1990). IBM created NetView to manage SNA networks, a de facto standard for operating SNA networks. NetView has an open architecture that permits the integration of other systems, but its strength is with SNA networks.

Both companies support open interfaces, common management features, a consistent user interface, and a common structure for management information (Jewell, 1990). Both IBM and DEC have introduced long-term, migration strategies in support of ISO standards and a more open architecture, so as to facilitate development of management products with interface capabilities to other vendors' equipment and management systems on the network.

The products developed around application-development platforms and proprietary systems are directed primarily to the Data and Transport Domains. These products are designed for managing network elements such as LAN bridges, routers, packet switches, and modems.

The third approach addresses full integration between the Data, Transport, and Voice Domains and use of equipment from multiple vendors. Examples include AT&T's Accumaster Integrator and NYNEX ALLINK Company's ALLINK Operations Coordinator products.

AT&T's overall architecture is called the Unified Network Management Architecture. Under this architecture AT&T offers a host of products designed to inter-work with UNMA in the management of different types of networks and services. The Accumaster Integrator is an example of one product that operates within the UNMA framework (Gilbert, 1990).

Both companies' products address management of equipment, networks, and services for both voice and data communications. Both companies' products also encompass management of carrier-provided services as well as customer-premises equipment and networks for data-communications. Examples include modems, multiplexers, LANs, host computers, and PBXs at the customer premises, along with local-exchange and inter-exchange networks and services. Both AT&T and NYNEX provide vendor-independent network management that requires application development for management of multi-vendor equipment. These management systems interface with various element management systems. Their varying levels of control include a single element (multiplexers, modems, hosts), a management system managing several elements (LAN managers), and management systems for carrier-provided, network services (Goleniewski and Horak, 1992).

4.6 Network Management Products Summary

The development of information with which to manage telecommunication resources (equipment and networks as well as the services that are provided) has been classified into five functional areas, summarized as

- **Fault Management:** the detection, isolation, and correction of abnormal network operation.
- **Accounting Management:** the accounting of, and subsequent charging for, all use of network resources.
- **Configuration Management:** the exchange of information between and control of various network resources in response to varying traffic and equipment conditions in the network.
- **Performance Management:** the evaluation of network resources in service to identify element and network degradation prior to a failure.
- **Security Management:** the control of access to network capabilities, and the handling of security-related information.

Information provided in accordance with these functional capabilities is used to satisfy four operational requirements: network operation, administration, maintenance, and planning and procurement (classified as provisioning by some organizations).

A recent survey of 300 information systems managers from 1,000 large companies indicates the three most important features of network management to be security, performance tracking, and rerouting capability. The bar graph in Figure 26 shows summarized results from the survey. However, monitoring and reporting of service degradation (a part of the performance management function) and remote testing and restoration of network resources (a part of the fault management function) are widely reported as among the most important aspects of network management.

Implementations of these management functions into hardware and software products with which to perform network management functions has occurred rather naturally in three separate domains that are convenient to follow in describing the scope of these management products. These are the Transport Management Domain, the Data Management Domain, and the Voice Management Domain. Within each domain, it has been convenient to divide management further into element-specific management and comprehensive element management. Many products are available today to manage specific resources that are used to provide specific services within each of the specific domains.

The report identifies and discusses many of the different viewpoints of integrated network management that are expressed today. Management capabilities that would monitor and control all telecommunication resources (network elements, networks, and communication services) in all three domains would be a logical example of truly integrated network management. Such capabilities, however, would require extensive management information databases, and utilization of the database information would consume considerable network bandwidth resources to exchange the necessary management information. Network management capabilities, integrated as just described, may be on the horizon, but such capabilities are not available today.

The discussion in Section 4.1 of network management domains leaves open the question of network management for ISDN. Such capability would provide yet another dimension of meaning to the term "integrated network management." However, standards for ISDN management capability are just beginning to be developed (see Question 9/II (CCITT, 1988)),

and there have not been strong user "demands" for such a capability. Therefore, products to provide ISDN management are not available yet.

The "integrated" management capabilities that are available include the following:

- Capabilities, or a platform upon which network management solutions are built and tailored to the network, to manage all resources that provide a particular service within a particular domain or across multiple domains. Such management capabilities and the resources managed are not restricted to the use of a particular architecture and may allow use of multiple vendors' equipment in providing the services—at least partially vendor-independent.

- Capabilities, designed around proprietary architectures such as the IBM System Network Architecture or DEC's DECnet architecture, to manage resources that may include equipment from multiple vendors for providing particular services within a particular domain or across multiple domains. Such management capabilities and the resources managed are restricted to the use of a particular architecture but still may allow use of multiple vendors' equipment in providing the services—again, partially vendor-independent.

- Capabilities that accommodate management across the data, transport, and voice domains and the use of equipment from multiple vendors, but that are limited to a particular network architecture. The Accumaster Integrator capability developed by AT&T that uses the Unified Network Management Architecture is an example.

5. HIGHLIGHTS, ISSUES, AND TRENDS IN NETWORK MANAGEMENT

The following subsections briefly describe highlights of this study along with an appraisal of the direction that the management of telecommunications networks appears to be going and some of the major issues that face the users and providers of these networks. No significance should be attached to the order of listing nor is any attempt made to distinguish between highlights, issues, and trends.

5.1 General

- We found network management to be an important but confusing subject. There appears to be no common, generally-accepted definition of network management. Some perceive network management as including everything except the actual transfer of user information. Others take a much more

limited point of view and assume network management deals only with traffic control in almost real time, providing congestion avoidance by alternate routing and related techniques. In this later case network management does not include, for example, the technical functions of service management often identified as administration, operation, and maintenance.

- The ISO/OSI provides functional definition for network management in their specification of five management functions—namely fault, configuration, performance, security, and accounting. These functions describe **what** the network is doing, **where** it is happening, **how** it is working, **who** is using it, and **when** it is being used.

- No network management systems are available that fully implement all of the ISO/OSI-defined functions. In fact, the management of networks from end-user to end-user is regarded as an unlikely capability in the near future, except for privately owned networks, due to administrative boundaries between customers' premises (equipment), local-exchange carriers, and inter-exchange carriers. Available management systems and products range from relatively simple LAN operation and control equipment to complex systems for managing nationwide (or international) networks. The growing number of different products and services, many of them vendor proprietary, are adding to the complexity of network management. A consistent, unified network management system based on common standards is a strategic issue that needs to be resolved.

- There is an increasing reliance on the public switched telephone network for government as well as business needs, due to its ubiquitous nature. It is a mistake to view network assets solely on the basis of an economic role and value; these assets also have national security and emergency communications value critical to the national welfare. Network management assets are of particular importance in network survivability.

- Common channel signaling technologies provide flexibility to network management but at the same time are vulnerable to multipoint failures in disaster situations. A backup system (e.g., communication satellites or other alternate network capability) might alleviate this situation.

- In retrospect, a major theme that we believe needs to be emphasized is that network management is a complex, confusing, and poorly-defined technology. And, there is much more work remaining to be done to develop ideal network management standards, systems, and products and to integrate all aspects of the technology so as to provide management on an end-to-end basis.

5.2 Standards

- Two principal areas of network management are being addressed in standards. One, called OSI management, deals with multilayered, network architectures that involve information processing and packet-switched data. These standards are primarily software oriented. The other, called telecommunications management, deals with telephone networks that involve circuit-switched voice and digital services provided by voice-bandwidth circuits. These standards are primarily hardware oriented. Future standardization efforts will address the integration of services that require network management integration of the OSI and telecommunications management structures for ISDN and B-ISDN. Thus, the trend is toward management of integrated architectures or the so-called information networks.

- Network management standards, as with many other types of standards, are usually not specified in sufficient detail to ensure full interoperability. Therefore, testing is required to insure that interfaces are compatible and all systems interoperate properly.

- The evolution of standards including network management standards is undergoing continuous change. Factors that influence this change include: new technologies, increasing numbers of competing suppliers of services and equipments, industry fragmentation in the United States as a result of divestiture, growing internationalization of networks and the European community's impact, national security implications, and the proliferation of high-speed data networks.

- The development of network management standards involves resolving conflicting interests in several areas. These include: public versus private domain interests, users' versus providers' interests, information-processing versus telephony interests, national versus international interests, and others.

- Three trends are expected to have major impact on the role of standards in the evolution and operation of public and private networks. These trends are: 1) increasingly complex technologies and services, 2) increasing users' demands for services, and 3) increasing numbers of suppliers of services and equipment, resulting in more competition.

- Modern networking facilities usually involve products that have been developed and marketed by numerous vendors. Because network management standards have not been completed, many proprietary management systems and implementations have evolved for use only with specific vendors' equipment. An important issue in managing integrated networks is the availability of standards that promote interoperability of

equipment and systems provided by multiple vendors and the portability of associated software. Network management standards that promote the creation of a multivendor environment, spanning multiple administrative areas, are essential. Eventually, as network management standards are enhanced and completed, proprietary implementations are expected to decrease.

- The United States Government has endeavored to develop standards for open systems interconnection and management of these networks (e.g., GOSIP and GNMP). Indeed, there is strong economic and interoperational justification for such standards being available and used in Government procurements. There needs to be more rapid convergence between these Government efforts and the other efforts to develop and promulgate standards for management of open interconnected systems and networks.

- A number of difficulties are encountered in developing international standards, including standards for network management, that need to be addressed. Solving complex technical problems is intrinsically difficult, but the technical difficulties are compounded by demands for interoperability in the modem, multivendor environments. This is especially true in the international arena because of various political interests and the large number of participants involved. Another factor is that the standards development process tends to be leading technology rather than just approving industry developments. This adds to the complexity of the process.

5.3 Technology

- Integrated network management systems of the future will monitor and control multimedia networks carrying audio, video, data, and text as in ISDN and B-ISDN.

- As technology advances into the gigabits per second range (e.g., fiber optics transmission), standards will be needed for these high-speed superhighways of digital information. Complex tests of entire systems, that include all network management functions, need to be developed and performed on an international basis.

- Management systems today are directed toward optimizing performance and availability of networks. In the future, intelligent systems should be designed for optimizing a network's efficiency and for adapting to users' changing needs as well as performing the conventional management processes. A user-supported approach, to complement the service providers' and equipment vendors' interests, has been missing from network management in the past.

- Broadband networks such as B-ISDN may be introduced progressively over the next decade or two. Broadband ISDN may be characterized as networks that support services requiring bit rates in excess of 1.5 Mb/s. Applications would include LAN and WAN interconnectivity, video telephony, and video conferencing. The asynchronous transfer mode (ATM) uses fixed-length packets (known as cells) for transferring digital information over a previously established virtual circuit. These cells are then multiplexed in time and sent over high speed transmission facilities using frames typically based on the synchronous digital hierarchy (SDH), e.g., SONET. Broadband ISDN introduces a whole new set of network management technologies and a corresponding number of issues. These may be addressed in future reports.

5.4 Market Forces

- Rapid access to information is a critical tool in today's competitive business world. Information networks are so important to the user that they do not want NM in third-party hands. Instead they often want interoperability with complete control of network functions and features on an automated basis. Therefore, users should be more involved in the standards making process.

- The importance of any network (data, voice, video, or information) stems from its use rather than anything inherent in the equipment and facilities. Benefits, in terms of increased services and revenues, are improved when systems are easier to use. Network management is an important factor in this implementation process for 'user-friendly' networking.

- A number of factors that are expected to cause major changes are impacting the communication market in 1992. These include new technology developments such as fiber optical transmission, broadband services, and personal communications systems. There is an increasing demand for better products at lower prices resulting in more innovation and production efforts by the telecommunications industry. Finally, there is the liberalization of the Postal Telephone and Telegraph (PTT) monopolies in Europe resulting in greater market potential for networks, the services provided by them, and the products used to manage them. All of these factors affect the market and, at the same time, impact network management systems.

6. CONCLUSIONS AND RECOMMENDATIONS

The information presented in this report is intended to satisfy three objectives:

- Identify and examine the confusion and diversity of understanding that exists today about the technology termed network management.

- Develop a conceptual definition and understanding of network management that is rational and comprehensive. Intentionally, the definition is not oriented exclusively to either data or voice networks; rather, it is suitable for all types of networks, including integrated-services networks, that provide a full range of telecommunication services.

- Examine the questions of what is involved in supporting and controlling these networks, what is being done or needs to be done to provide that support and control, and who is involved in doing it.

Directed to these objectives, the report (1) presents a conceptual explanation of network management that purposely is somewhat idealistic; (2) describes the many organizations that are active in the development of real-world, network-management standards and the contribution that each is providing; (3) examines the functional characteristics of a variety of current network management products, including some examples; and (4) discusses some of the important issues and trends that are creating challenging new requirements for network management.

There is no common definition of network management that is widely accepted. A variety of definitions and perceptions, reflecting the views of providers, users, standards organizations, and developers and vendors of hardware and software for network management, are discussed in Section 1. The following general definition is presented:

> **Network management is the act or art, more or less skilled, of supporting and controlling an interconnected group of communicating entities and nodes (e.g., telephones, terminals, computers, circuits, and switches).**

Fundamental concepts of network management are developed in Section 2. This development considers network management to be a management process that applies to all of the telecommunication resources, including the network, the network elements, and services provided by the network, independent of any specific network architecture.

The functions that need to be performed through the process of network management are examined in Section 2. Five functional areas have been defined by the International Organization

for Standardization that are widely accepted by users, providers, and standards-making organizations:

(1) fault management—what is the network doing?

(2) accounting management—when is the network used?

(3) configuration management—where is everything in the network?

(4) performance management—how is the network doing?

(5) security management—who can use the network?

Conceptual approaches for designing this functional management capability include centralized network management, distributed network management, and hierarchical network management. These different approaches to network management are not exhaustive, but form the basis for specific implementations that combine these conceptual approaches in many ways. These implementations are consistent with the network architecture that is required to provide the features that are important to the network providers and users.

Admittedly, these concepts for network management are idealistic. There are numerous factors that must be taken into account as network management standards are developed and management practices and systems that conform with the approved standards are developed and implemented. Extensive information concerning standards for network management is presented in Section 3 and Appendix A.

The development of standards for network management has produced at least four rather separate groups or types of standards:

(1) Standards for which the development work has been coordinated and approved by the IAB. The SNMP (and an associated Management Information Base) for the Internet and other TCP/IP networks is the most familiar. (The IAB also is directing development of a framework for common management information services and protocols that are compatible with the ISO/OSI-based standards. CMOT is the principal network management product from this effort.)

(2) Proprietary "standards" developed by individual companies or organizations. These standards often have been accepted for a time as de facto standards. Examples include SNA used by IBM, the OpenView network architecture used by HP, and the DECNet architecture used by

Digital Equipment Corporation. Fortunately, most of the companies that have been developing and using these proprietary standards now are attempting to be compatible and interoperate with equipments and systems that conform with either the SNMP/CMOT or CMIS/CMIP standards, or both.

(3) Standards that are developed by a diverse support base and ultimately endorsed and adopted by national and international organizations with wide influence, such as CCITT, OSI, groups that are accredited by the American National Standards Committee, the OSI Network Management Forum, and others. Familiar examples for network management include the CMIS and CMIP and an associated MIB that are based on the OSI Reference Model. In addition, the CCITT has defined International Network Management, for telephone service including ISDN, and the Telecommunication Management Network that include definitions of many management functions.

(4) Standards developed by the United States Government. Although not fully implemented at this stage, OSI-based standards have been recommended for use in procuring network management products by the Federal Government. The Government Network Management Profile (NIST, 1991), as a companion standard to GOSIP, is an example.

The SNMP and associated MIB are criticized by many as being too limited in the capabilities offered for network management. Proponents and users of SNMP argue, however, that it is available now, it works, and it provides an adequate capability that satisfies their current requirements for network management.

The emerging international and open-systems standards are broad, not entirely consistent, and, often-times, too general. These characteristics cause difficulty when attempting to develop and market network management products that conform to the standards. Despite the efforts of organizations like the Corporation for Open Systems and the European Standards Promotion and Applications Group to overcome these problems with the international standards, there still tends to be reluctance by both users and product developers to attempt to conform with the standards. This reluctance exists because the generality and lack of consistency in standards mean there is no guarantee that products from different developers and vendors will interoperate or provide exactly the same functionality.

The positive side of international standards, however, is that such standards do promote system interoperability through conformance to open network architecture objectives, and the

standards are supported widely outside of the United States. In addition, the international standards, generally speaking, have greater functional capability than most other standards, for example, the Internet standards. These points are discussed more completely in Section 3.

The telephone company was the first and essentially exclusive network manager. Later, as data communications networks developed and opportunities to provide new services were recognized following divesture of the Bell System, the requirements and capabilities for network management expanded. These were, and continue to be, evolutionary processes that first provided simple management for individual elements of the network. As the number and type of elements increased and "the network" became more complex, the requirements for and complexity of network management systems also increased.

Implementations of the management functions described earlier into hardware and software products with which to perform network management have occurred rather naturally in three separate domains, the Transport Management Domain, the Data Management Domain, and the Voice Management Domain. The development of products has been divided further within each domain into element-specific management products and comprehensive element management products. Many products are available today to manage specific telecommunication resources that are used to provide specific services within each of the specific domains.

This report introduces and discusses several current viewpoints on integrated network management (Section 2). However, management capabilities that would monitor and control all telecommunication resources (network elements, networks, and communication services) in all three domains would be an example—logically—of fully integrated network management. But, such capabilities would require extensive management information databases, and utilization of the databases information would consume considerable network bandwidth resources to exchange the necessary management information. Fully integrated network management capabilities may be on the horizon but are not available today.

The earlier definition of three network management domains leaves open the question of network management for ISDN. Such capability would provide yet another dimension of meaning to the term "integrated network management." However, standards for ISDN management capability are just beginning to be developed, and there have not yet been strong user "demands" for such capability. Therefore, products to provide ISDN management are not available yet.

The "integrated" management capabilities that are available today include

- Capabilities to manage multiple vendors' equipment, generally used within a single domain (voice, data, or transport) to provide a particular service. The "platform" approach is used to tailor network management to a particular network without restrictions to particular architectures.

- Capabilities designed in accordance with proprietary architectures (such as IBM's SNA or DEC's DECnet) to manage multiple vendors' equipment, generally within a single domain (voice, data, or transport) to provide a particular service.

- Capabilities that manage multiple vendors' equipment in multiple domains, where there is restriction to a particular network architecture. The Accumaster Integrator capability that conforms to the Unified Network Management Architecture, developed by AT&T, is an example.

The development of standards for network management and inter-operability of the network management systems is an integral and essential part of the evolutionary processes for developing and marketing management products. However, a reality in all of this is that increased synergy among the standards, widespread conformance with the standards, and the ultimate capability of truly integrated network management with systems inter-operability will occur only as it becomes economically viable. Users of TCP/IP and SNMP, for example, are likely to continue to request SNMP products to manage their data networks as long as such products are the least expensive and satisfy their management requirements. Products that conform with ISO/OSI standards for interoperability and integrated network management will be developed and available to users only as developers and vendors perceive an economically-viable demand. That demand will arise only when managers recognize their existing management capabilities to be inadequate to satisfy their (increasing) requirements and when such products are available at reasonable cost.

Both favorable and unfavorable influences arise from market competition and telecommunication regulation on the development of network management standards and systems. Competition continually stimulates the development of new and innovative technology that benefits users with more and easier-to-use products and services at competitive prices. There is debate, however, concerning the effectiveness of competition in assuring high reliability for these products and services. Competition may influence a developer to market a product before it has

been thoroughly tested. Proponents argue that some regulation may be necessary to assure acceptable reliability.

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 influences and may restrict their willingness to completely and cooperatively support the agreements that would provide for ideal standards that would be completely consistent and sharply focused.

7. REFERENCES

ANSI (American National Standards Institute) (1983), American National Standard for Information Systems — Data Communication Systems and Services — User-Oriented Performance Parameters, ANSI X3.102-1983, approved February 22 (American National Standards Institute, Inc., 1430 Broadway, New York, NY 10018). (Also adopted as Federal Standard 1033 and FIPS-PUB-144.)

ANSI (1989a), American National Standard for Telecommunications T1.204 — Operations, Administration, Maintenance and Provisioning (OAM&P) — Lower Layer Protocols for Interfaces Between Operations Systems and Network Elements.

ANSI (1989b), American National Standard for Telecommunications T1.208 — Operations, Administration, Maintenance and Provisioning (OAM&P) — Upper Layer Protocols for Interfaces Between Operations Systems and Network Elements.

ANSI (1989c), American National Standard for Telecommunications T1.210 — Operations, Administration, Maintenance and Provisioning (OAM&P) — Principles of Functions, Architectures and Protocols for Interfaces Between Operations Systems and Network Elements.

ANSI (1989d), American National Standard for Telecommunications T1.204 — Operations, Administration, Maintenance and Provisioning (OAM&P) — Generic Network Model for Interfaces Between Operations Systems and Network Elements.

ANSI (1990), A methodology for specifying telecommunications management network interfaces, Technical Subcommittee T1M1.

Aronoff, R., M. Chernick, K. Hsing, K. Mills, and D. Stokesberry (1989), Management of networks based on open systems interconnection (OSI) standards: functional requirements and analysis, NIST Special Publication 500-175, November (National Computer Systems Laboratory, National Institute of Standards and Technology, Gaithersburg, MD).

Axner, D.H. (1990), Digital's strategy: enterprise management architecture, *Networking Management,* May, p. 52.

Bartee, T.C. (1989), *ISDN, DECnet, and SNA Communications,* Chapter 7, (Howard W. Sams and Company, Indianapolis, IN).

Bellcore (1989), *Network Management Handbook, Network Planning and Engineering Series* (Bell Communications Research, Inc., 290 W. Mt. Pleasant Ave., Livingstone, NJ 07039-2729).

Ben-Artzi, A., A. Chandra, and U. Warrier (1990), Network management of TCP/IP networks: present and future, *IEEE Network Magazine,* July, pp. 35-43.

Beyltjens, M., J. Cornille, R Falkner, and B. Panigas (1989), Telecommunications management networks, *Electrical Communication 63,* No.4.

Böhm, W., and G. Ullmann (1989), Network management, *Electrical Communication 63,* No.1.

Bryan, J.S. (1991), PCN: prospects in the United States, *Telecommunications,* January, pp. 54-56.

Callahan, B. (1991), Modems: market overview, technology overview, and comparison columns (with Barbara Rinehart), Datapro Reports on Data Communications (McGraw-Hill, Inc., Datapro Research Group, Delran, NJ), C33-010-101, C33-010-201, and C33-010-301, March.

Cargill, C.P. (1989), *Information Technology Standardization; Theory, Process, and Organizations* (Digital Press, Bedford, MA).

Caruso, RE. (1990), Network management: a tutorial overview, *IEEE Communications Magazine,* March, pp. 20-25.

Case, J.D., M.S. Fedor, M.L. Schoffstall, and J.R. Davin (1989), A simple network management protocol (SNMP), Univ of Tennessee at Knoxville, NYSERNet, Rensselaer Polytechnic Inst., and MIT Lab. for Computer Science, RFC 1098, April.

Cassel, L.N., C. Partridge, and J. Westcott (1989), Network management architectures and protocols: problems and approaches, *IEEE Journal on Selected Areas in Communications 7,* No.7, September, pp. 1104-1114.

CCITT (International Telegraph and Telephone Consultative Committee) (1988), International network management, Question 9/II, Questions Allocated to Study Group II (Network Operation) for the 1989-1992 Study Period, Study Group II — Contribution 1, Document COMM II-I, December, pp. 14-15.

CCITT (1989a), Terms and definitions, Blue Book Vol. I, Fascicle I.3, IXTH Plenary Assembly, Melbourne, November 14-25, 1988.

CCITT (1989b), International network management — general information, Recommendation E.410; operational guidance, Recommendation E.411; controls, Recommendation E.412; planning, Recommendation E.413; and organizations, Recommendation E.414, Blue Book Vol. II, Fascicle II.3, pp. 5-34, IXTH Plenary Assembly, Melbourne, November 14-25, 1988.

CCITT (1989c), Various recommendations pertaining to international telephone and data networks and ISDN, Blue Book Vols. II, III, IV, VI, and VIII, IXTH Plenary Assembly, Melbourne, November 14-25, 1988.

CCITT (1989d), Principles for a telecommunications management network, Recommendation M.30, Blue Book Vol. IV, Fascicle IV.1, pp. 22-61, IXTH Plenary Assembly, Melbourne, November 14-25, 1988.

CCITT (1989e), Reference model of open systems interconnection for CCITT applications, Recommendation X.200, Blue Book Vol. VIII, Fascicle VIII.4, pp. 3-56, IXTH Plenary Assembly, Melbourne, November 14-25, 1988.

CCITT (19890, Network management administration, Recommendation Z.337, Blue Book Vol. X, Fascicle X.7, IXTH Plenary Assembly, Melbourne, November 14-25, 1988.

COS (Corporation for Open Systems) (1987), COS protocol support, Version I, Corporation for Open Systems, COS/SFOR 87/0004.01.

Datapro (1991), LAN and internetwork management systems: overview, Datapro Reports on Network Management Systems (McGraw-Hill, Inc., Datapro Research Group, Delran, NJ), NS30-010-101, January, pp. 101-120.

Desikan, D. (1990), Bringing strategic value to network management systems, *Telecommunications,* December, pp. 60-62.

Embry, J., P. Manson, and D. Milhan (1991), *Interoperable Network Management: OSI/NM Forum Architecture and Concepts, Integrated Network Management II,* I. Krishan and W. Zimmer (Editors) (Elsevier Science Publishers, B. W. North Holland), p. 29.

Feridun, M., M. Lieb, M. Nodine, and J. Ong (1988), ANM: automated network management system, *IEEE Network 2*, No.2, March.

Flanagan, W. (1990), The proper scope of network management, *Telecommunications,* August, pp. 43-45.

Frank, H. (1988), The real network management problem, *Business Communications Review,* July-August, pp. 35-38.

Freeman, R.L. (1989), *Telecommunication System Engineering*, Second Edition (John Wiley and Sons, New York, NY).

Gawdun, M. (1987), Customer-controlled network management, *Telecommunications*, July.

Gilbert, W.E. (1990), Managing networks in a multi-vendor environment, *IEEE Communications Magazine*, March, pp. 41, 42, 59, and 60.

Goldsmith, S. and U. Vizcaino (1989), Enterprise network management, integrated network management, Proceedings of the IFIP TC 6WG 6.6 Symposium on Integrated Network Management, Boston, MA, Vol. I, May 16-17, pp. 541-552.

Goleniewski, L., and R. Horak (1991), Telemanagement systems and software: market overview, Datapro Reports on Network Management Systems (McGraw-Hill, Inc., Datapro Research Group, Delran, NJ), NS60-010-101, September, pp. 101-108.

Goleniewski, L., and R. Horak (1992), NYNEX ALLINK Co. ALLINK operations coordinator, Datapro Reports on Network Management Systems (McGraw-Hill, Inc., Datapro Research Group, Delran, NJ), NS20-674-101, March, pp. 101-107.

Gove, P.B., Editor-in-Chief (1976), *Webster's Third International Dictionary of the English Language* (G. & C. Merriam Company, Publishers, Springfield, MA).

GSA (General Services Administration) (1991), Telecommunications: Glossary of Telecommunication Terms, Federal Standard 1037B, approved June 3 (published by the General Services Administration, Office of Technology and Standards, Washington, DC 20407).

GSA (1986), Glossary of Telecommunication Terms, Federal Standard 1037A, approved June 26 (published by General Services Administration, Office of Information Resources Management, Washington, DC 20407).

Herman, J. (1989), What is network management and why is everybody talking about it?, *Business Communication Review*, February, pp. 81-83.

Hewlett Packard (1989), HP OpenView Network Management Server, Technical Data Bulletin.

IEEE (Institute of Electrical and Electronic Engineers) (1990a), 802.1B draft standard: LAN/MAN management, Network Management Task Group, IEEE 802.1 Working Group, March.

IEEE (1990b), 802.1F Draft recommended practice: guidelines for the development of layer management standards, Network Management Task Group, IEEE 802.1 Working Group.

ISO (International Organization for Standardization) (1984), International Standard 7498-1, Information Processing Systems — Open Systems Interconnection — Basic Reference Model (Secretariat ISO/IEC JTC1/SC 21—American National Standards Institute, 1430 Broadway, New York, NY 10018).

ISO/IEC (1989), International Standard 7498-4, Information Processing Systems — Open Systems Interconnection — Basic Reference Model — Part 4: Management Framework (Secretariat ISO/IEC JTC1/SC 21—American National Standards Institute, 1430 Broadway, New York, NY 10018).

Jander, M. (1991), Network management systems get to work, *Data Communications,* July, p. 47.

Jay, F., Editor-in-Chief (1988), *IEEE Standard Dictionary of Electrical and Electronics Terms*, ANSI/IEEE Std 100-1988, Fourth Edition, July 8 (published by The Institute of Electrical and Electronics Engineers, Inc., New York, NY).

Jewell, B.R (1990), An insider's view: IBM's network management architecture, *Journal of Network Management*, Summer, pp. 11-19.

Joseph, C.A., and K.H. Muralidhar (1990), Integrated network management in an enterprise environment, *IEEE Network Magazine,* July, pp. 7-13.

Knight, I. (1991), Telecommunications standards development, *Telecommunications,* January, pp. 38-40.

Knightson, K.G., T. Knowles, and J. Larmonth (1988), *Standards for Open Systems Interconnection* (McGraw-Hill Book Company, New York, NY).

Linfield, R.F., and M. Nesenbergs (1985), Military access area characterization, NTIA Report 85-185, November (NTIS Order No. PB 86-148855, 5285 Port Royal Road, Springfield, VA 22161).

Linfield, R.F. (1990), Telecommunications networks: services, architectures, and implementations, NTIA Report 90-270, December (NTIS Order No. PB 91-151852/LP)

Llana, A. (1990), Managing corporate networks, Datapro Management of Telecommunications (McGraw-Hill, Inc., Datapro Research Group, Delran, NJ), MT70-200-101, August, pp. 101-117.

Marney-Petix, V. (1992), Network management capabilities of LAN NOSs, Datapro Reports on Network Management System (McGraw-Hill, Inc., Datapro Research Group, Delran, NJ), NS30-020-101, March, pp. 101-105.

McCloghrie, K., and M. Rose (1988), Management information base for network management of TCP/IP-based internets, RFC 1066, The Wollongong Group, August.

Mitchell, T. (1991), What is the most important feature of network management?, *Network World,* December 23, p. 13.

Nesenbergs, M. (1991), Simulation of hybrid terrestrial-satellite networks for service restoral and performance efficiency, NTIA Report 91-281, November (NTIS Order No. PB 92-143460/AS)

NIST (National Institute of Standards and Technology) (1991), Government network management profile (GNMP), Version 1.0, (Preliminary review copy), March 8 (National Institute of Standards and Technology, Building 225, Room B217, Gaithersburg, MD 20899).

OSI/Network Management Forum (1990), Release 1 Specifications, Forum 001 — Forum 009 (OSI/Network Management Forum, 40 Morristown Road, Bernardsville, NJ 07924).

Pyykkonen, M. (1989), Network management: end-user perspectives, *Telecommunications,* February, pp. 23, 24, and 72.

Rey, R.F. (Technical Editor) (1983), *Engineering and Operations in the Bell System,* Second Edition (AT&T Bell Laboratories, Murray Hill, NJ).

Ricci, S.G. (1991), PBX systems: technology overview, Datapro Reports on Telecommunications (McGraw-Hill, Inc., Datapro Research Group, Delran, NJ), TC07-001-201, April, pp. 201-209.

Rose, M.T. (1988), ISO presentation services on top of TCP/IP-based internets, RFC 1085, The Wollongong Group, December.

Rose, M.T. (1991), *The Simple Book, An Introduction to Management of TCP/IP-based Internets* (Prentice Hall, Englewood Cliffs, NJ).

Rose, M., and K. McCloghrie (1988), Structure and identification of management information for TCP/IP-based internets, RFC 1065, The Wollongong Group, August.

Su, D.H., and L.A. Collica (1991), ISDN conformance testing, Proc. IEEE, Vol. 79, No. 2, February, pp. 190-198.

Terplan, K. (1989), Integrated Network Management, Proceedings of the Network Management and Control Workshop, September 19-21, 1989, Tarrytown, NY, pp. 31-57 (Edited by Aaron Kershenbaum, Manu Malek, and Mark Wall and Published (1990) by Plenum Press, 233 Spring Street, New York, NY 10013).

Valovic, T. (1987), Network management: the state of the art, *Telecommunications,* July, pp. 45-55.

Warner, J. (1991), Moving toward OSI-based network management systems, *Network Management,* May, pp. 56-58.

Wetmore, R.S. (1991), The evolution of network management at AT&T, *Telecommunications Journal* 58, No. VI, June, pp. 366-369.

Willets, K. (1991), Developing Concert™ for open, integrated network management, *Telecommunications*, February, pp. 63-66 and 72.

Willitts, K. (1988), A total architecture for communication management, Proceedings of the International Conference on Network Management, London, pp. 59-71.

Womack, A. (1990), An overview of telephone management systems and software, Datapro Management of Telecommunications (McGraw-Hill, Inc., Datapro Research Group, Delran, NJ), MT60-210-101, September, pp. 102-106.