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 (1989), may be somewhat out of date in terms of the status column, but it does indicate the extent of recent activities in network management.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.

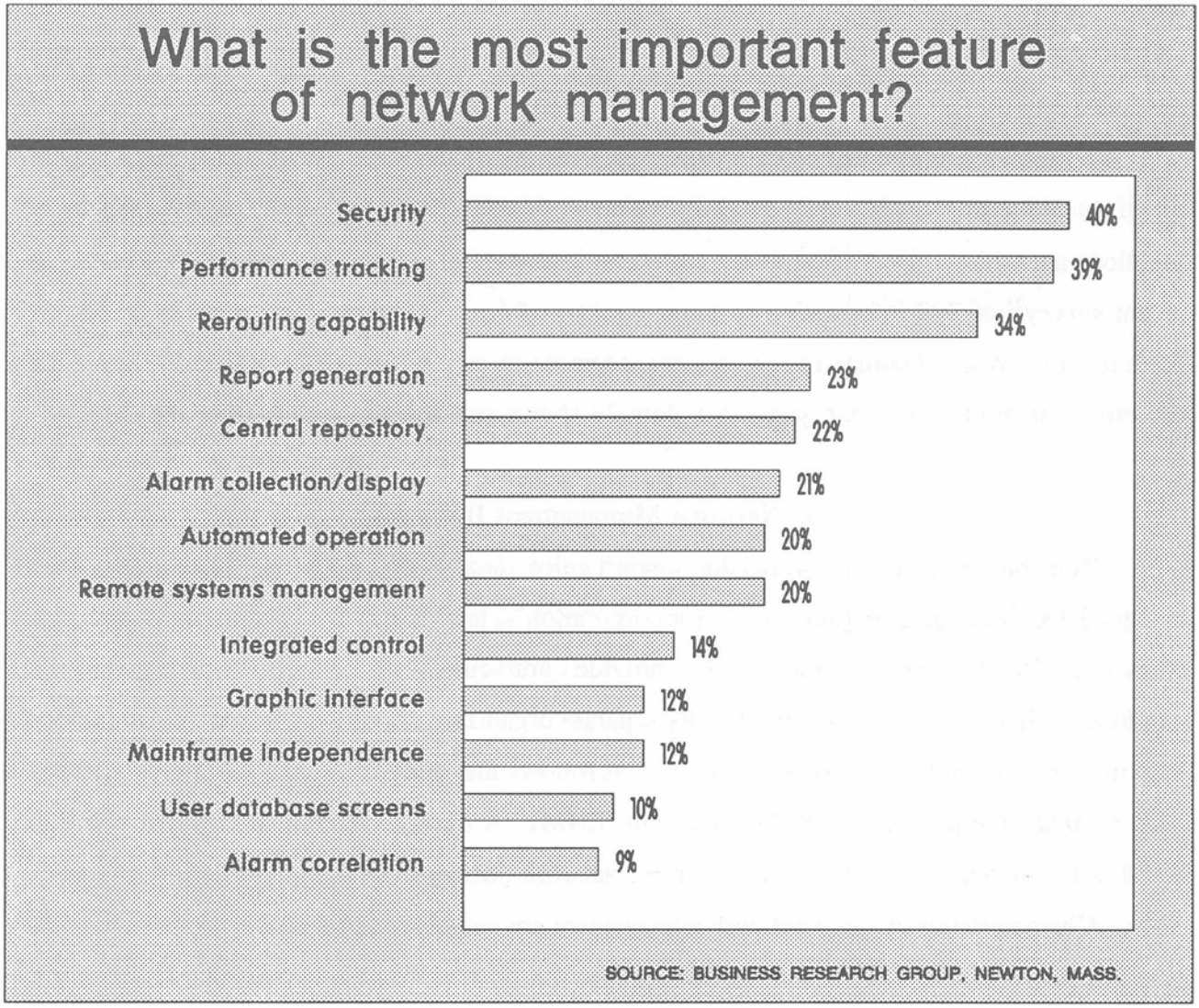

Figure 26. Results indicating most important features of network management (for local networking) (based on original graphic by Mitchell, 1991).

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.

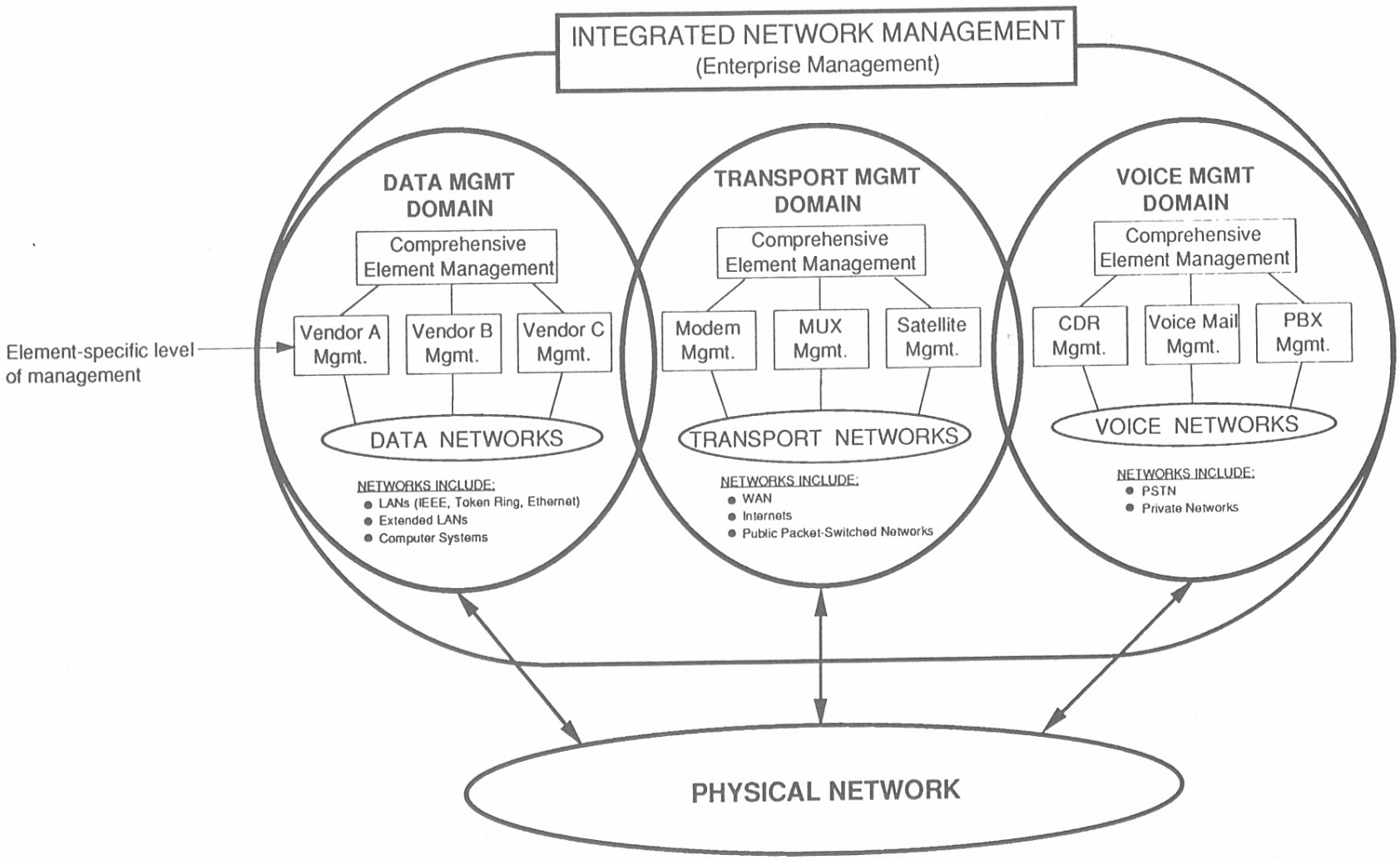

Figure 27. Network management domains showing hierarchical management architecture within each domain.

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

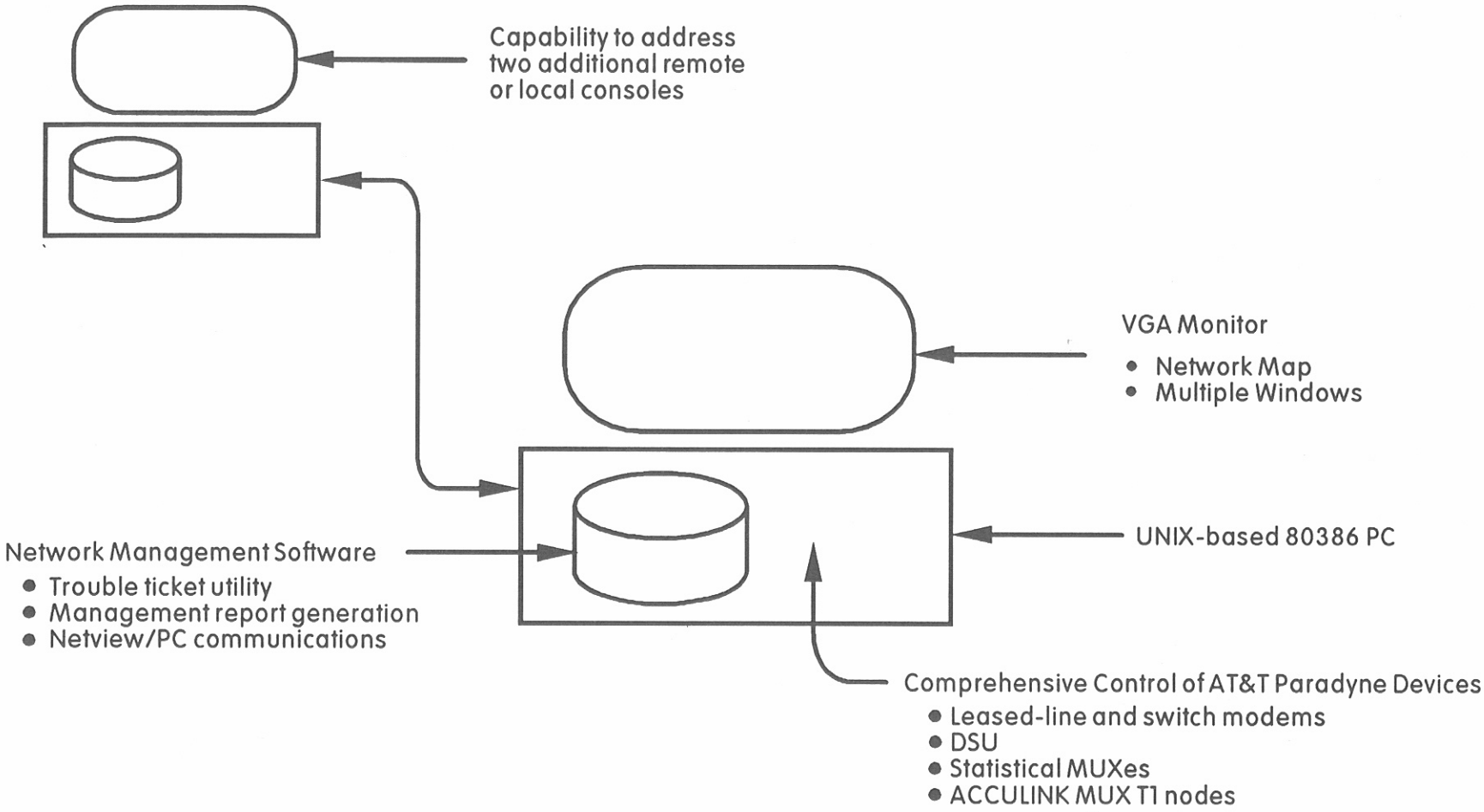

Figure 28. Example of a comprehensive network management system--AT&T Paradyne Comsphere 6820 Network Management System.

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.

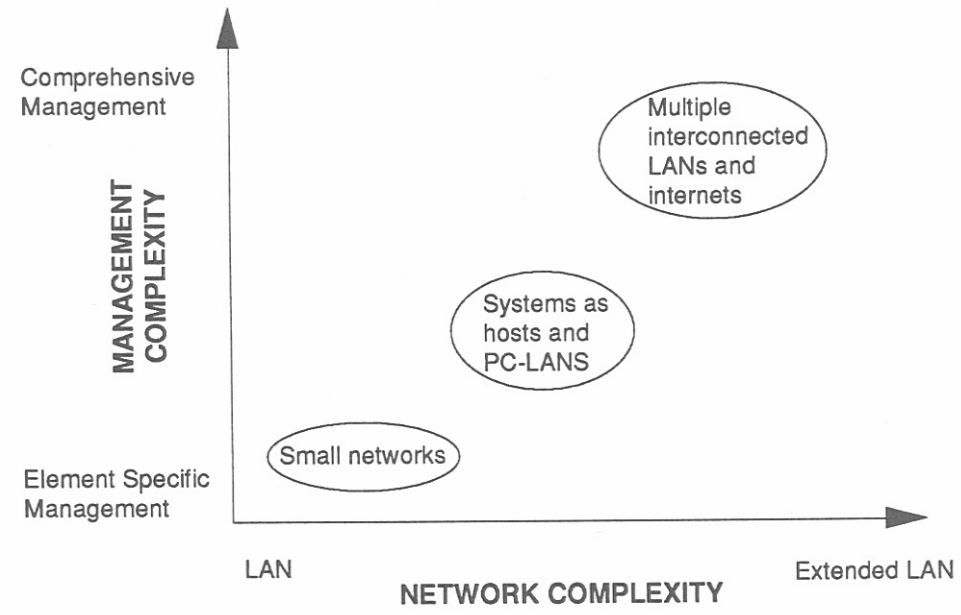

Figure 29. Management complexity as a function of network complexity.

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

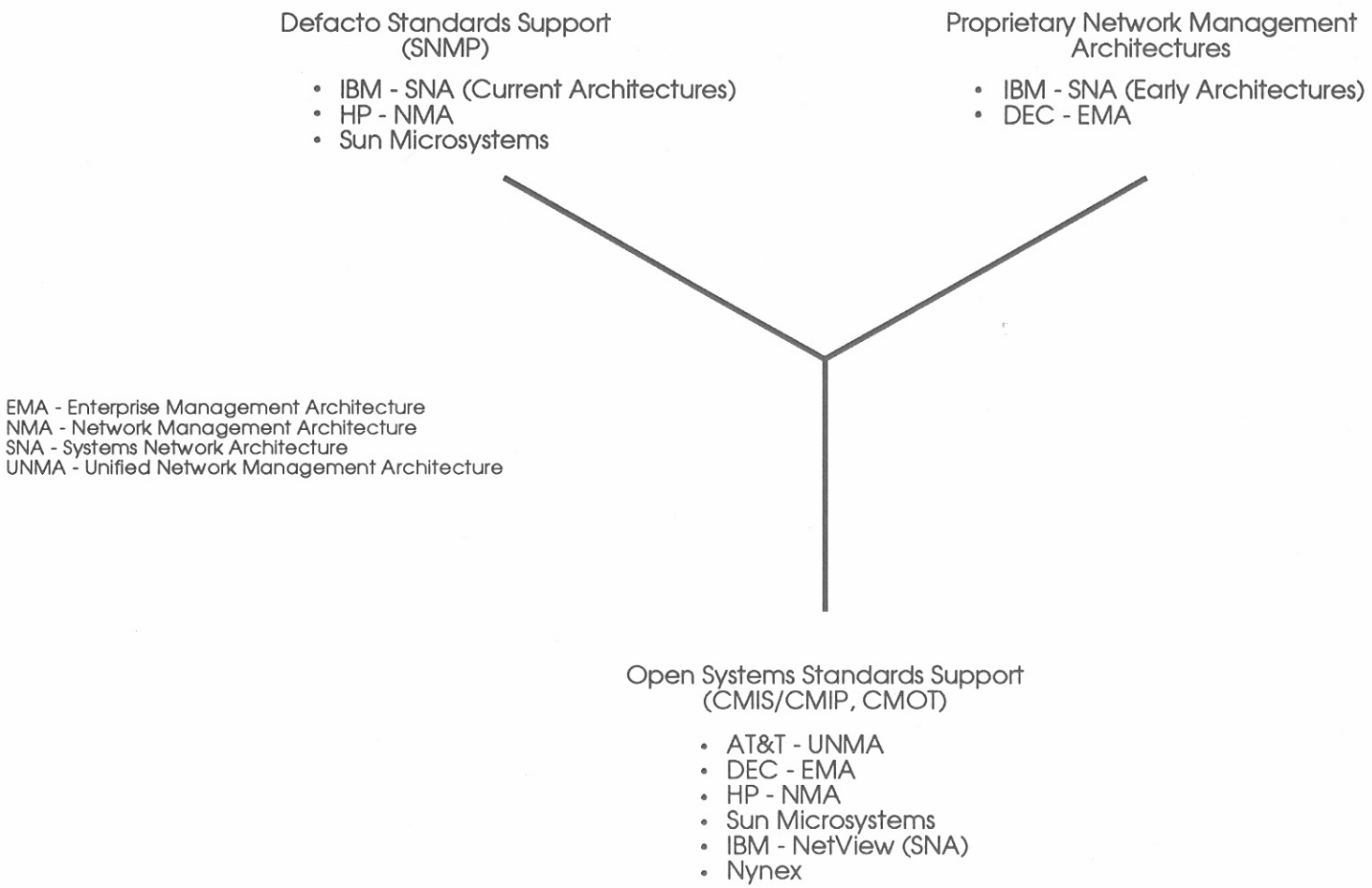

Figure 30. Examples of various vendors' support to network management standards.

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.