CHAPTER 1

Principles of Network Management

Salah Aidarous
NEC America
Irving, TX 75038

Thomas Plevyak
Bell Atlantic
Arlington, VA 22201

1.1 INTRODUCTION

Telecommunications networks have become essential to the day-to-day activities of the enterprise and individuals. Many corporations, agencies, universities, and other institutions now rely on voice, data (e.g., facsimile transmission, electronic funds transfer), and video (e.g., video teleconferencing) services to ensure their growth and survival. This trend will accelerate as personal communications services (PCS), LAN-to-LAN interconnectivity, image file transfer, and other innovative services are developed and are standardized throughout the operation of the enterprise.

In parallel with rapid advances and increased reliance on telecommunications services, network technologies continue to evolve. For example, transport technologies, such as the synchronous optical network (SONET), will support asynchronous transfer mode (ATM) and frame relay to deliver broadband services at both constant and variable bitrates. Innovative access technologies are emerging to accommodate customer-premises equipment access to higher bandwidth services and an expanding range of mobility services (e.g., PCS), and to provide seamless access to fiber optic and satellite networks. In addition, the advanced switching technologies required for ATM technology and switched multimegabit digital service (SMDS) are now being deployed.

Network management is one of the most important yet confusing topics in telecommunications today. It includes operations, administration, maintenance, and provisioning (OAM&P) functions required to provide, monitor, interpret, and control the network and the services it carries. These OAM&P functions provide operating telephone companies (OTCs) and their corporate customers and end-users with efficient means to manage their resources and services to achieve objectives. There have been different approaches and strategies taken by OTCs, equipment vendors, and users to manage their networks and equipment. Management solutions are often specific to each vendor's networking product environment.

Traditionally, the public network was designed to handle voice and data services using both analog and digital technologies. Network management methods were introduced according to each technology and service. The outcome was multiple overlays of circuit-switched, packet-switched, and slow-switched connectivity nodes. Private networks, on the other hand, were built to provide enterprise information networking using PBXs, mainframes, terminals, concentrators, and bridges. The public network was used to provide the wide area backbone network. From an OAM&P perspective, interoperability between these networks has been a major challenge for the telecommunications and computing industries.

Figure 1-1 shows a typical enterprise network that includes both the private corporate data network (usually managed by the corporate telecommunications group) and the public part of the corporate network which is usually managed by the OTC and the interexchange carrier (IEC). PBXs may also be owned and managed by the OTC. The network may carry different services that require different management methods and may cross jurisdictional boundaries involving different management organizations [1].

As the pace of technological development quickens, new products are brought to market even faster and support of several generations of equipment and software is required. The current network environment is complex, diverse, competitive, and characterized by different service subnetworks, multiple overlays, and multiple media. These factors have increased the cost of network management (e.g., operations costs are exceeding capital costs) making it the primary concern of many corporations, OTCs, equipment suppliers, and standards organizations.

This chapter addresses overall principles of network management. In that sense, it is an overview, not intended as introductory material to other chapters. Instead, Chapters 2 and 3 are tutorial and introductory. This book focuses on telecommunications OAM&P and network management. Data network management is treated where relationships overlap, but this area is not a central focus.

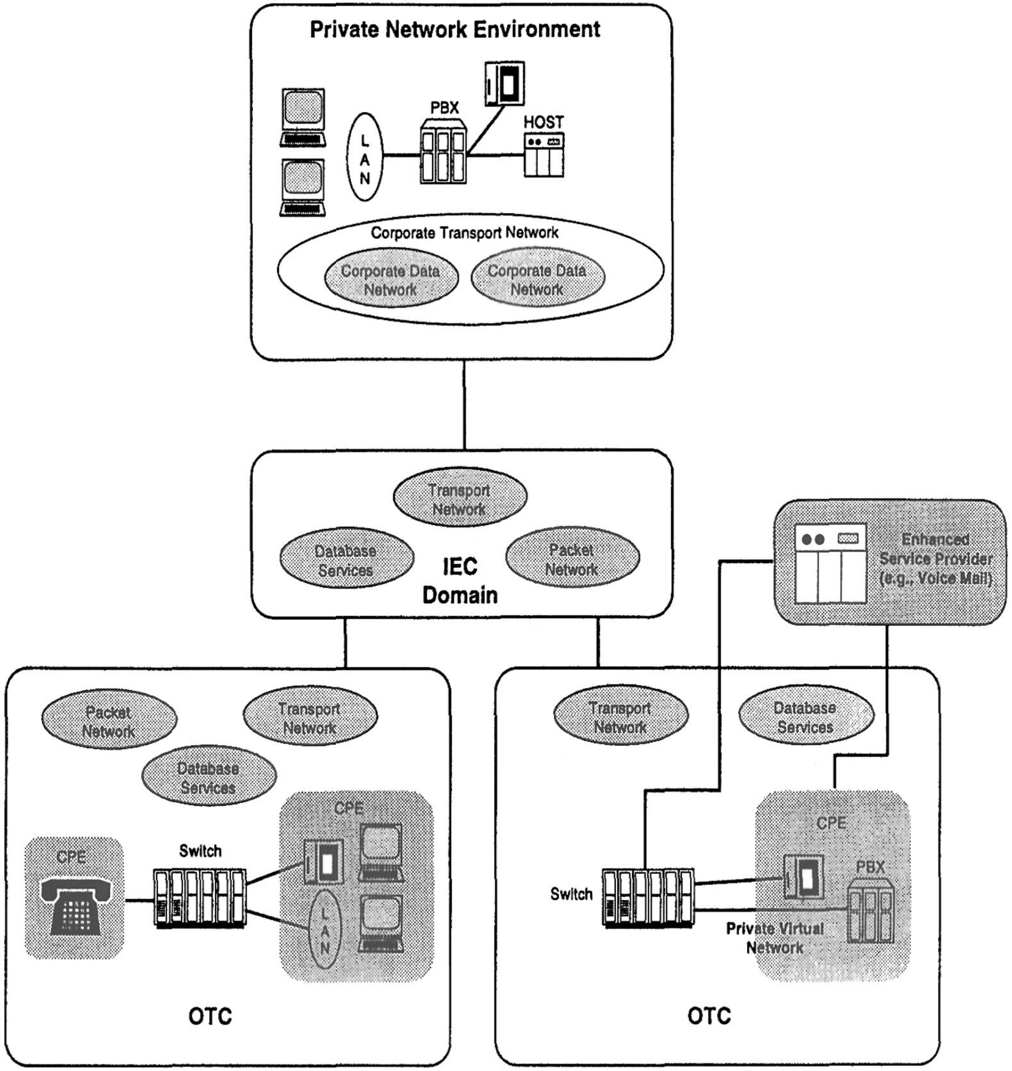

Figure 1-1 Typical Network Configuration

1.2 DRIVERS FOR NETWORK MANAGEMENT

In today's dynamic telecommunications environment, changes are occurring on many fronts. Services and network technologies are advancing rapidly, competition among service providers is intensifying, and customer demand for network access and customized services is increasing. A fundamental means of achieving these desirable changes is through an evolution of existing network management architectures [2].

Services Evolution: Network end-users are employing a spectrum of increasingly "complex" services that range from low-speed, bursty services to high-speed, continuous services and to high-bandwidth pay-per-view video. Conversely, large- and medium-business customers desire simpler, cheaper, yet even higher bandwidth services to link LANs for video conferencing and to enable effective information networking and distributed computing. They also want the consolidation of data, voice, image, and video traffic on their enterprise networks. New services are being developed at an ever-quickening pace. For example, virtual private network services are provided as an alternative to dedicated facilities. Personal communications services will provide the subscriber accessibility to his or her telephone services as well as reachability through a single telephone number.

Technology Evolution: Network technology is undergoing consolidation. For example, integrated circuit, frame, and packet switches, capable of carrying all services, is achievable with current technology. Coupling narrowband ISDN (basic and primary rate) and broadband ISDN provides a consolidated set of access technologies. On the other hand, SONET transport systems will provide a consistent digital core network. This is augmented on the private network side by integrated PBX technologies, LANs that carry all services, and use of high bandwidth services to consolidate wide area traffic. Network technology evolution is exploiting recent advances in distributed systems technology [open software foundation (OSF), distributed computing environment/distributed management environment (DCE/DME), telecommunications management network (TMN) [3-4], telecommunications information networking architecture/information networking architecture (TINA/INA)[5]], internet technology [extended internet protocol (IP), simple network management protocol (SNMP)], database driven services systems [advanced intelligent network (AIN)], and radio access systems.

Customer Requirements: Business customers are pushing for bandwidth- and service-on-demand with electronic interfaces to the network for requesting services or changes, reporting troubles, billing, and making payments. They want provisioning times in the order of minutes and services that do not fail. Residential customers and corporate network end-users want to set up basic or enhanced services such as call management or custom local area signaling system (CLASS), when and where they want them, through a simple, one-step process.

Competitiveness: The competitive landscape is changing for network/service providers. Business pressures are forcing many service providers to find ways to reduce operations costs, use resources more efficiently, streamline the implementation of new services and technologies, and identify new revenue-generating opportunities. Private network operators wish to use their networks as strategic elements in their own business areas but are being forced to reduce overhead wherever possible. These pressures will increase in the future.

Considering the rapid deployment of new services and technologies, escalating competitive pressures, and the broadening demands of customers, service providers face an immediate and pressing need to streamline, simplify, and automate network management operations.

1.3 TRADITIONAL APPROACHES TO NETWORK MANAGEMENT

Today's telecommunications networks (see Fig. 1-2) are characterized by a tight coupling of specific services to specific network resources, typically deployed in a series of multiple overlays; multiple OAM&P networks and operation systems for each of these service and resource overlays; and organizational structures made up of separate groups performing similar functions. This duplication of overlay structures was related to the operational characteristics of older technologies. In addition, specific vendor elements had their own proprietary approaches to OAM&P and network management created multiple administrative domains with poor interoperability between them. The total was the sum of all these independent, resource consuming partial solutions that have contributed to a network management environment that is inefficient, complex, and expensive to administer.

Traditional network management practices deal with a wide array of procedures, processes, and tools for configuration, fault detection, performance monitoring, security, accounting, and other management functions and are based on a "master–slave" relationship between management or operations systems[1] (OSs) and network elements (NEs). Network ele-

[1] The terms operations systems (OSs) and network management systems (NMSs) are used interchangeably in this book.

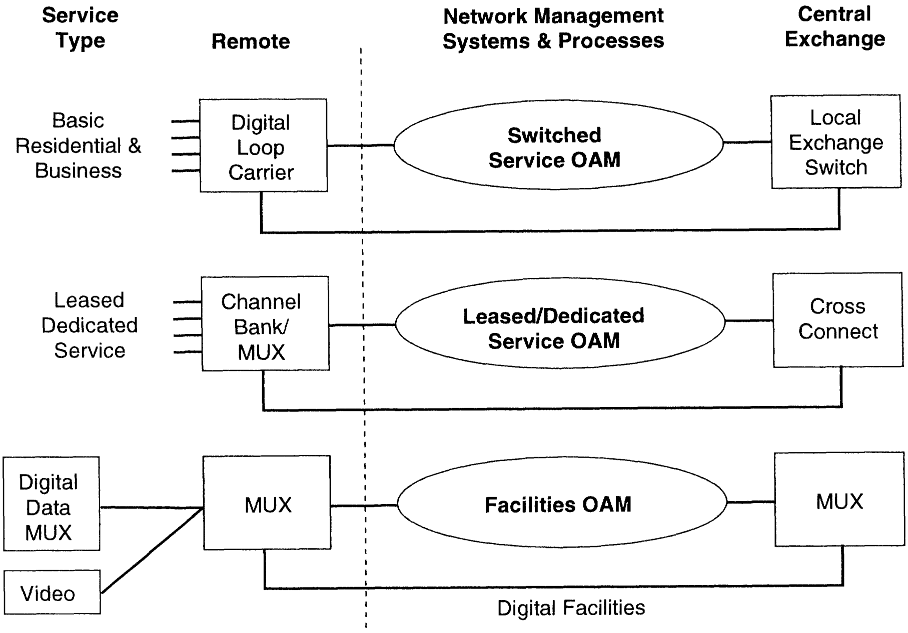

Figure 1-2 Current Service-Resource Relationship

ments typically have had only basic operations functionality with little ability to control activities or make decisions beyond the scope of call processing and information transmission. Accordingly, operations systems perform the bulk of the OAM&P work—processing raw data provided by individual network elements, making decisions, and instructing each individual network element to undertake specific actions.

This master–slave relationship contributes to operating inefficiencies in a number of ways. For example, there is little sharing of logical resources, such as data, because network elements and operations systems have been designed independently. In addition, each vendor's equipment has unique configuration and fault management interfaces as well as specific performance requirements. Network management systems must characterize each network element and vendor's interfaces on an individual basis, adding considerable time and complexity in introducing new services or technologies.

Other factors have compounded this complexity. For example, network management systems were generally constructed to optimize the work of individual service provider organizations or work groups at a particular point in time for a particular suite of technology. This type of development was undertaken independently by each organization and little attention was paid to system level interworking. Many copies of data, each tied to specific systems or job functions and to specific equipment vintages or implementations, were incorporated throughout the network, creating a major data synchronization problem. As a result, it has become increasingly difficult for the service provider, as a whole, to evolve services, network technologies, and network management processes in a cost-effective, timely, competitive manner in response to rapid changes in the telecommunications business.

1.4 REQUIREMENTS FOR AN EVOLUTIONARY NETWORK MANAGEMENT ARCHITECTURE

In developing an evolutionary network management architecture that will overcome the inefficiency, costliness, and complexity of the existing environment, it is essential to address key service, technical, and business aspects.

Service aspects include:

- enabling rapid new service deployment within both the network and network management system environments and
- promoting faster service activation.

Management or operations systems must be flexible and have a distributed, modular architecture that allows service providers to adapt to future customer needs. These needs may include, for example, rapid service deployment and activation, enhanced billing, and end-user online feature access. New software and features should ensure that customer services can be added in minutes rather than days or weeks.

Technology aspects include:

- the challenge of efficiently managing and distributing data throughout the network and
- elimination of physical overlay networks currently required for service/resource deployment and associated management systems.

Data management represents a major cost item for service providers due to the volume, redundancy, and difficulty in ensuring accuracy throughout a network/service provider's operation. Therefore, evolutionary architecture should allow for distribution of data throughout all layers of the network management environment and provide for intelligent network elements that can process data and pass information to network management systems on a peer-to-peer basis. Manual administration and alignment of redundant databases should be eliminated.

Given the sophistication and rapid growth of services, a more flexible operations environment must be established (i.e., multiple, single-function overlay networks must be eliminated). A distributed operations environment that correctly uses the capabilities of all components will remove the current interoperability bottleneck resulting from the proliferation of overlay networks.

An important step in creating this flexibility is to eliminate discrete overlay networks, by introducing network technology capable of providing generic resource capacity. This capacity will be logically assigned to a broad range of service types (i.e., the network will be provisioned in bulk and the services will be logically assigned to the network resources). Furthermore, incorporating intelligent network elements in the evolving operations architecture and repartitioning operations functions between network elements and network management systems will add momentum to the process of decoupling network management from service- and vendor-specific implementations. Successful achievement of this objective will be dependent upon utilization of standard open interfaces (covered in more detail in Chapters 2 and 3).

Business aspects include:

- reducing operations costs,
- enhancing the flexibility of the OAM&P environment, and
- providing services in a competitive, timely manner.

Cost reduction can be addressed on a number of fronts. One means is through simplifying the network, i.e., replacing service and technology-specific resources with generic resources capable of carrying a wide range of services. For example, replacing plesiosynchronous transport with SONET technology will reduce the need to manage multiplexors. In the access domain, software-controlled service-adaptive access technologies (e.g., those that enable service characteristics to be electronically downloaded to the network element) will simplify the network further and reduce the frequency and complexity of personnel dispatches. Another means of reducing cost is by integrating and simplifying operations processes and functions. Cost/benefit can also be achieved through elimination of redundant databases and amalgamation of processes and work forces so that these align with the network/service provider's business objectives. In addition to streamlining functions and costs, another benefit is an improvement in service responsiveness and quality. This could be achieved by providing near real-time service provisioning, automatic service restoral in the event of network disruption, and just-in-time resource provisioning.

An important means of enhancing OAM&P flexibility is to incorporate more intelligence into network elements. This redistribution of management functionality will enable network management systems to maintain a high-level, end-to-end view of services and resources (as opposed to the current scenario in which management systems must understand the implementation details of each individual network element's technology).

For network and service providers, this flexibility will mean that today's organizationally based operations structures and systems will move to a functionally based structure that spans a variety of services and technologies. One operations group could manage network surveillance, for instance, across all access, transport, and switching domains rather than having different surveillance groups for each domain. This distribution of functionality and data closer to the point of origin and application will pave the way for a simplification of operations systems and enable centralization of the operations workforce. Currently, many service providers are redesigning their business processes, an activity known as *process reengineering,* to achieve major gains in costs and services.

An evolutionary architecture should accomplish the overall objective of providing manageable flexibility points between the network management system, services, technologies, and service provider organizational structures. Experience has shown that services, technologies, and organizational structures traditionally evolve at independent rates; a modular operations architecture will facilitate each evolutionary step without necessitating a complete system redesign—a redesign that typically impacts each area highlighted in Fig. 1-3.

Future architectures are intended to guide the evolution of the existing network management environment to an advanced infrastructure that will enable service providers to achieve their business objectives and satisfy their long-term requirements for systems and organizational change. As illustrated in Fig. 1-4, future architectures orchestrate interactions

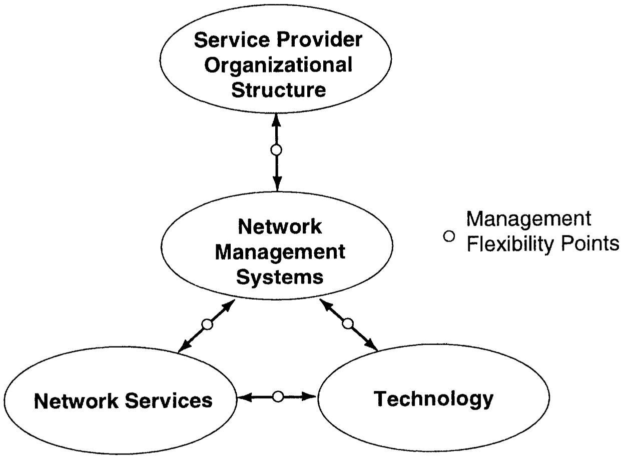
Service Provider Organizational Structure
Network Management Systems
Management Flexibility Points
Network Services
Technology

Figure 1-3 Network Management System Relationships

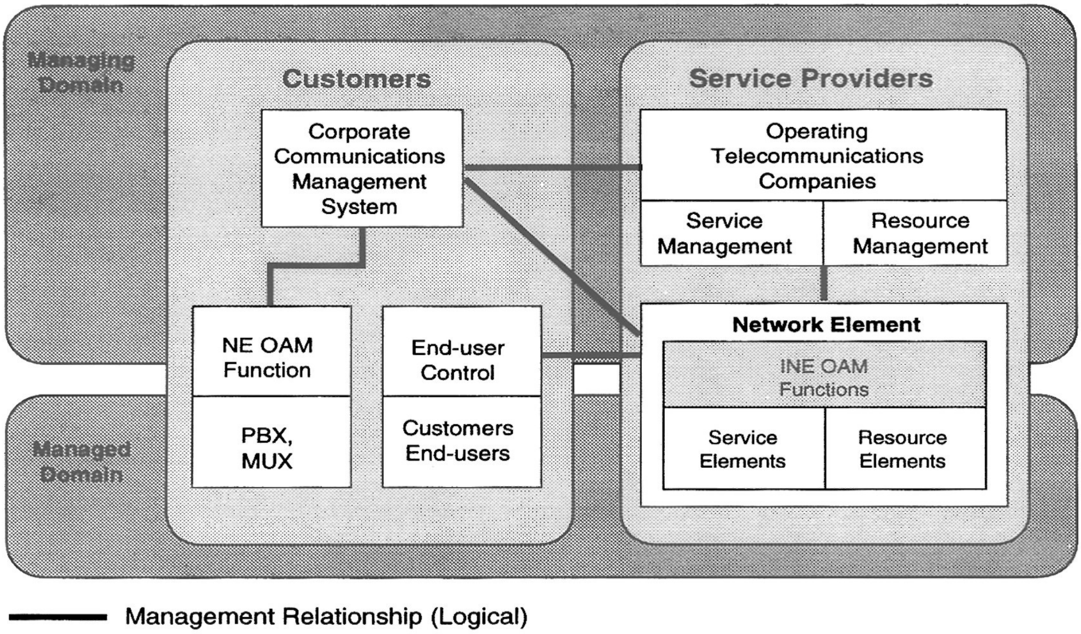

Figure 1-4 Network Management Domains

between the operations environment (comprising network management systems and intelligent network elements) in the managing domain and the base network elements in the managed domain. As well, the network management environment must also accommodate management requirements of corporate customers and individual end-users.

The OAM&P managing domain includes:

1. *Service provider's network management systems* that ensure a combined end-to-end view of the network for both service and resource management and reflect the primary business objectives of the service provider;
2. *Intelligent network elements* that have control applications capable of translating standard high-level messages from the network management applications to the vendor-specific technology implementations;
3. *Corporate communications management systems* for private networks. These systems provide corporate customers with functionality similar to network/service provider management systems (service and resource management, inventory management, directories, cost allocation, and traffic reports). Corporations currently have limited control over the services received from the public network provider. However, network/service provider service revenues could be increased by providing more

public network services to the corporate users if the services could be managed by the users in a secure and responsive manner; and

4. *Extended control functionality* that permits management of services and features by the *end-users,* either in conjunction with, or independent of, a corporate communications management system. These control functions could also enable residential or small business customers to modify their service profile directly from their terminals. The network element management function would update the service provider's network management system autonomously; increasing the customer involvement will reduce costs and improve responsiveness.

Both managing and managed domains are concerned with network service and resources. A key consideration is that the development of the interface between network management systems and the intelligent network element (INE) functions in a manner that does not stifle change or cause unnecessary disruption. For example, managed services typically span multiple versions of a single vendor's technology, not to mention technology from multiple vendors. Interfaces should change only if service capabilities evolve, not simply because a vendor's implementation changes.

In implementing the basic OAM&P architecture, the following requirements will be satisfied:

- communications will be established between network management systems and intelligent network elements;
- services will be managed as independently as possible from the resources on which they are implemented; and
- functional applications software will be incorporated within INEs to permit the mapping of generic high-level standard messages onto vendor-specific implementations.

Communications between network management systems and network elements will be standardized across vendor-specific implementations through a high-level open system interconnection (OSI) reference model (see Chapter 5), compliant with the TMN established by the International Telecommunications Union—Telecommunications (ITU-T—formerly CCITT) [4]. The reference model describes a communications architecture into which standard protocols, containing a clear description of data and data structures, can be placed or defined. Moreover, the model addresses the syntax and transfer of information and attempts to standardize the modeling and semantics of management information.

In addition to implementing a common communication framework that will ensure operations system and network element cooperation across OSI interfaces, the emerging management environment will incorporate functional applications that reside within the intelligent network elements. These functional applications will play a variety of roles from managing data to provisioning services to sectionalizing problems within specific network elements or transmission facilities.

For instance, each INE can be configured to steward its own data and to provide complementary OAM&P functionality to the network management systems. By optimizing data distribution and ensuring that the intelligent network element is able to autonomously update the network management systems on an as-required basis, operations performance is enhanced and redundant data is eliminated [6].

The architecture also provides for sharing of common supporting functions between OAM&P applications and the network management functional areas (i.e., OAM&P data management or security management). In addition, sharing of common functions applies to the complementary implementation in the network elements. This approach promotes consistency in implementation and minimizes development costs.

Prerequisites for data management include:

- ensuring accessibility of OAM&P data to multiple management applications;
- collecting and maintaining data from multiple sources;
- flexibility in aligning and synchronizing data; and
- management of data consistency between the network element data and the redundant or local copies, where necessary.

Additional requirements to be addressed in the emerging management systems include providing partitioned and secure data storage, OAM&P applications data views, OAM&P data formatting, and data alignment mechanisms.

Security management deals with protecting OAM&P applications, functions, and data against intentional or accidental abuse, unauthorized access, and communications loss. Security management can be implemented at different levels, including network provider and customer groups, network management systems, OAM&P applications, or functions and objects (see Chapters 4 and 5). User profiles, specifying access privileges and capabilities, will be based on hierarchical levels of authorization that reflect each group's administrative structure.

As customers place more stringent demands on the reliability and performance of the network, combined with the service provider's need to achieve more with the same number of or fewer people, the requirement for greater flexibility in assigning levels of access security increase. If the entire customer control issue can be considered to be an extension of the operations environment, partitioning of network management access—whether to a management system or directly to a network element—will simply be a matter of restricting access to their own service profiles and customer groups.

1.5 NETWORK MANAGEMENT FUNCTIONS

Architecture and control systems are key for evolving today's limited network management systems to meet tomorrow's objectives. Customers, as shown in Fig. 1-5, will have access to service providers' network management systems and applications. By repositioning network databases to take advantage of intelligent network elements, providing high-level standard interfaces, implementing standard protocols and messages, and sharing OAM&P functionality across operations systems and intelligent network elements, the evolving network will enable network/service providers to rapidly deploy new services, implement innovative technologies, reduce costs, enhance competitiveness, and meet the ever-increasing demands of customers.

This vision of an intelligent network will ultimately be realized in the telecommunications management network (TMN)[3], a management communications concept that defines the relationship between basic network functional building blocks (operations systems, data communications networks, and network elements) in terms of standard interfaces. The TMN also introduces the concept of subnetwork control that will play a pivotal role in evolving today's limited network management systems to meet future business objectives. A subnetwork is an aggregation of a group of NEs tied together by a common criteria (e.g., function, technology, supplier), and is viewed by the management application as a single entity. A device that implements subnetwork OAM&P functionality, known as element manager (EM), is an instrumental building block that will simplify the interworking between operations systems and network elements [7]. From an architectural perspective, EM provides the flexible management point between network management systems and the vendor implementation of technology. It uses the TMN framework for communications management with its generic information models and standard interfaces.

Behind the vision of an intelligent network lie a number of key tasks, including functional partitioning, high-level object-oriented messaging, autonomous updating or notifying, and functional applications, all of which must be performed effectively.

From a network management perspective, standards bodies address

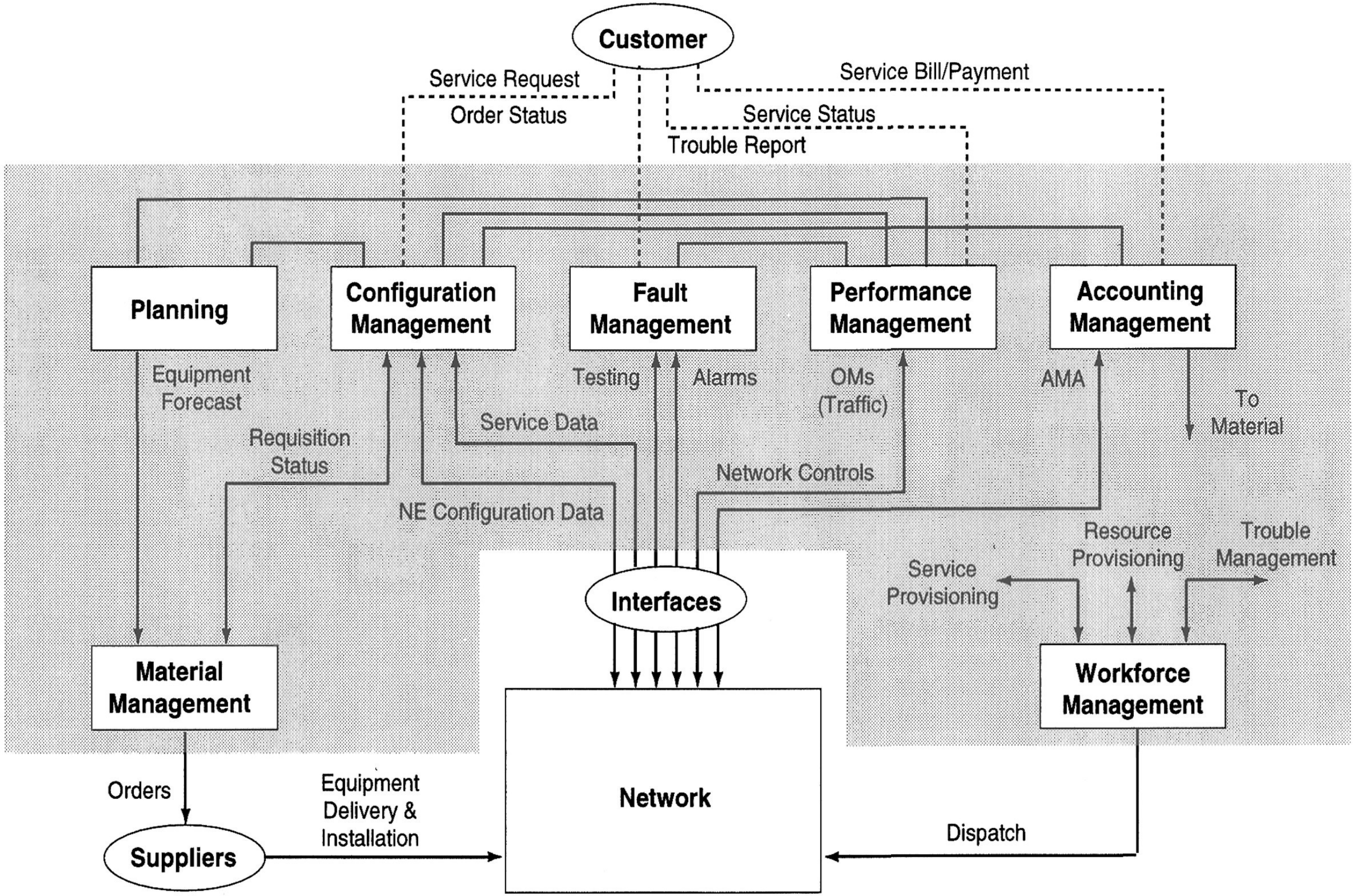

Figure 1-5 Network Management Functions

five functional areas, each of which represents a set of activities performed by operations personnel or customers. In many cases, both the network management system and the intelligent network element are involved in completing the functional task. Operations are separated from technologies by defining generic OSI-based OAM&P functions that are common to multiple technologies and services:

- *Configuration management* includes resource provisioning (timely deployment of resources to satisfy the expected service demand) and service provisioning (assigning services and features to end-users). It identifies, exercises control over, collects data from, and provides data to the network for the purpose of preparing for, initializing, starting, and providing for the operation and termination of services. Configuration management deals with logical, service, or custom networks such as the toll network, local public switched telephone network (PSTN), and private networks.

- *Fault management* includes trouble management, which looks after corrective actions for service, fault recovery, and proactive maintenance, which provides capabilities for self-healing. Trouble management correlates alarms to services and resources, initiates tests, performs diagnostics to isolate faults to a replaceable component, triggers service restoral, and performs activities necessary to repair the diagnosed fault. Proactive maintenance responds to near-fault conditions that degrade system reliability and may eventually result in an impact on services. It performs routine maintenance activities on a scheduled basis and initiates tests to detect or correct problems before service troubles are reported.

- *Performance management* addresses processes that ensure the most efficient utilization of network resources and their ability to meet user service-level objectives. It evaluates and reports on the behavior of network resources and at the same time ensures the peak performance and delivery of each voice, data, or video service.

- *Accounting management* processes and manipulates service and resource utilization records and generates customer billing reports for all services rendered. It establishes charges and identifies costs for the use of services and resources in the network.

- *Security management* controls access to and protects both the network and the network management systems against intentional or accidental abuse, unauthorized access, and communication loss. Flexibility should be built into security mechanisms to accommodate ranges of control and inquiry privileges that result from the variety of access modes by operations systems, service provider groups, and customers who need to be administratively independent.

Configuration management, fault management, and performance management are discussed in detail in Chapters 8, 9, and 10. Security management is treated in Chapter 4.

There are also several important network management functions that are not currently being addressed by standards or other forums, even though they are part of the conceptual framework:

- *Planning* encompasses the set of processes that permit the timely installation of resources to specify, develop, and deploy services in the network in response to service provider forecasts and end-user requirements.

- *Workforce management* plans and controls the activities of operations personnel. It deals with all workloads, personnel, and tools used in the management of the network. This includes repair (fault management), installation and cable locating (service provisioning), cable splicing and switch installation (resource provisioning), and field and central office technicians.

- *Material management* is concerned with procurement, control, and storage of equipment used in the installation and repair of the network. Material acquisition includes search, selection, and commitment of supplies and equipment from certified vendors. Material control monitors and updates inventory to ensure availability of material when and where required. Material distribution includes the handling of equipment from vendors and operations personnel, and the appropriate and timely delivery to the final destination.

Functional partitioning involves grouping functions into building blocks whose implementation can be moved across traditional boundaries in the physical architecture. Partitioning is essential to achieve effective, automated information flow-through on a complete system scale. This contrasts with today's approach in which attention is directed to isolated pockets of mechanization. Partitioning is also required in system development so that manageable portions of the operations architecture can be identified and allocated to specific projects.

Information models provide an abstraction of the telecommunications resources to be managed in the form of generic or technology-independent managed objects. To provide common solutions for switching and transport OAM&P, ITU-T has also generated an initial generic network information model in Recommendation M.3100 [4]. A key benefit is that this information model enables autonomous update and notification between the managed domains so that operating companies can provide corporate and, potentially, residential end-users, with immediate, independent access to services.

1.6 TRANSITION

The challenge facing network/service providers is how to manage the change in a continuously evolving network. Target architectures are being defined to support information networking services that will span multiple networks using equipment from several suppliers. Transition to these target architectures requires orchestrated automation, re-engineering of business processes, and introduction of new technologies. Transition strategies and alternatives need to be evaluated using prototyping, modeling, and simulation tools (see Chapters 6 and 7).

Realizing such hybrid environments is a large and complex undertaking with many challenges. Major advances in distributed data management, system platforms, interfaces, and security are needed in order to realize these challenges.

1.7 ORGANIZATION OF THE BOOK

Chapters 2 through 7 address new concepts and tools for network management. Chapter 2 describes network management problems, the different paradigms for network management, and provides a critical assessment for these directions. Chapter 3 defines the telecommunications management network (TMN) principles, associated implementation architectures, and applications. Chapter 4 provides an overview of OSI management activities within domestic and international standards forums. Chapter 5 provides a detailed overview of the object-oriented paradigm and its application to network management. Chapter 6 identifies the role of modeling and simulation in network management. Chapter 7 describes knowledge-based systems and applications to network management.

Chapters 8 through 11 deal with specific network management applications and their evolution as a result of these new concepts and paradigms. Chapter 8 describes configuration management and some associated network planning aspects. Chapter 9 provides a functional description of fault management and the associated interface specifications. Chapter 10 covers performance management and quality of service. Chapter 11 describes fast restoration techniques for high-speed networks.

REFERENCES

[1]. S. E. Aidarous, D. A. Proudfoot, and X. N. Dam, “Service Management in Intelligent Networks,” IEEE Network Magazine, vol. 4, no. 1, January 1990.

[2]. D. A. Proudfoot, S. E. Aidarous, and M. Kelly, “Network Management in an Evolving Network,” ITU - Europa Telecom, Budapest, October 1992.

[3]. CCITT, “Principles for a Telecommunications Management Network,” M.3010, 1992.

[4]. CCITT, “Generic Network Information Model,” M.3100, 1992.

[5]. Bellcore SR-NWT-002268, “Cycle 1 Initial Specifications for INA,” issue 1, June 1992.

[6]. Bellcore TA-STS-000915, “The Bellcore OSCA Architecture,” issue 3, March 1992.

[7]. Bellcore TA-TSV-001294, “Framework Generic Requirements for Element Management Layer (EML) Functionality and Architecture,” issue 1, December 1992.