Joe Ghetie et al. "Network Management and Administration"
The CRC Handbook of Modern Telecommunications
Ed. Patricia Morreale and Kornel Terplan
Boca Raton, CRC Press LLC. 2001

3

Network Management and Administration

Joe Ghetie
Bellcore

Kornel Terplan
Industry Consultant and Professor

Endre Szebenyi
Industry Consultant

Takeo Hamada
Fujitsu Laboratories America

Hiroshi Kamata
OKI Electric

Stephanie Hogg
Telsta Research

Carel Marsman
CMG

Introduction

It is not enough to develop, implement, and rollout new technologies by telecommunications service providers. These technologies should be properly administered and managed. Over a five-year period, management and administration would take up to 85% of operating expenses; acquiring the technology, just 15%. It is a very important metric for cost-justifying investments into management and administration.

This segment addresses administration and management issues. Management concepts outline the basics of managers and managed entities. Concepts include several management models, such as central and decentral, concentrated and distributed, and the use of hierarchical schemes supported by umbrella managers. Also, open management is addressed, including the open systems conceptual model, associated systems concepts, and requirements for open management systems. Distribution of management processes and functions will play a key role in future management solutions. Managed entities must be connected with element managers and management platforms using in-band or out-of-band communication schemes. This contribution gives examples for both alternatives.

Administration and management are usually an afterthought when considering the deployment of innovative technologies. This contribution tries to bring the technology deployment with the selection and implementation of management solutions into synchronization. Each technology that is considered innovative, such as frame relay, FDDI/CDDI, Switched MultiMegabit Data Service (SMDS), ATM, Sonet/SDH, Cable, mobile and xDSL, is investigated for how far management and administration solutions are available and implementable. In particular, the availability and structure of MIBs (management information base) are analyzed. In most cases, MIBs support most of fault, configuration, performance, security, and accounting management functions. MIBs in combination with SNMP managers do useful work for history-type of data visualization, analysis, and reporting. State-of-the-art technology needs additional management tools and applications that help with real-time decision support.

Management and administration depend to a large extent on management standards. There are two principal groups: standards for enterprise-level administration and management, and standards for

specific telecommunications environments. The management standards contribution focuses on enterprise-level standards, such as SNMP, RMON, and DMI, first. Components of telecommunications standards are also discussed in some depth, e.g., CMIP, Corba, and DCOM. This contribution prepares the readers for telecommunication network management (TMN) and Telecommunications Information Networking Architecture (TINA), and for better understanding management framework products and management applications.

TMN is a very simple model for streamlining management and administration. It uses four layers in addition to the network element's layer at the bottom. Management processes, fucntions, and tools may be categorized in accordance with these layers. This TMN contribution goes into depth and discusses various TMN models (information, fucntional, and physical), TMN elements (operations systems function, workstation functions, mediation functions, Q adapter function, network element function), TMN internal and external interfaces (Q3, Qx, X, F, and M), and the most appropriate use of Data Communication Network (DCN).

TINA goes one step behind TMN and offers four dimensions of considerations: life cycle management, computational infrastructure, partitioning by layers and domains, and functional representing fault, configuration, accounting, performance, and security management. TINA and TMN can work together, but they are not identical. TINA puts more weight on service fulfillment and service assurance. Also, resources are described in much more depth. TINA can be tailored to the needs of particular service providers.

The TeleManagement Forum offers guidance for deploying and re-engineering telecommunications business processes. This contribution uses the basic business model of breaking down support processes into two dimensions: life cycle of services, such as fulfillment, service assurance, and billing processes, then hierarchy of services, such as customer care processes, service development and operations processes, and networks and systems management processes. This contribution handles all 16 principal support processes, individually. Also, their links to each other, to the customers, and to the physical networks are addressed.

Management frameworks are the heart of support systems for telecommunications providers. They consist of an application platform and of management applications. This contribution outlines the principal attributes, such as architecture, application programming interfaces, protocol support, hardware and software platforms, graphical user interface, application programming interfaces, management functions supported, security modules, modeling capabilities, and internal systems services. For both telecommunications and enterprise environments, framework products are listed, and a few of them, such as OpenView from Hewlett-Packard, TNG from Computer Associates, FrontLine Manager from ManageCom, NetExpert from Objective Systems Integrators, and TeMIP from Compaq/Digital are analyzed in some depth. Over the next couple of years, frameworks are expected to embed the best of suite management applications with the result of full functionality to implement operations, business, and marketing support systems.

It is expected that telecommunications service providers and their customers will connect their management systems and applications. The name of this concept is customer network management (CNM). This contribution outlines the joint work, principal management processes and functions, and also legal issues. If successful, information exchange between providers and customers can be accelerated, and duplicated functions can be eliminated.

Service management is in the center of the next contribution. Service quality may be improved when certain management functions are outsourced to third parties. This contribution details the drivers for outsourcing and critical success factors of outsourcing alliances. Reporting on principal services metrics is key in all relationships. This contribution deals with practical examples for performance indicators and service level reports. Service management means more than element management. Service management is targeting more consolidated metrics in the TMN architecture.

Web technology is going to change the way management and administration systems work. Using Java applets and components of Web-Base Enterprise Management (Wbem) standards, management and

administration can be unified and simplified. This contribution handles Web basics (URL, Web server, Web browser, HTML, XML, and HTTP), evolving standards (Java and Wbem), and many application examples from framework vendors and management application vendors. This technology is expected to penetrate and change the way present operations, business, and marketing support systems work.

Support systems of telecommunications providers represent a very complex but increasingly significant segment of the communications industry. This contribution starts with the market drivers for support systems, such as network complexity, customer in focus, more standards, very high growth rates, deregulation, and convergence, followed by startegical benefits of such support systems. This contribution also identifies the suppliers of support systems, such as consulting companies, computer manufacturers, equipment manufacturers, software companies, and outsourcers. The remaining part of this contribution focuses on positioning products in terms of supporting markets (voice, data, Internet, cable, and wireless), supporting management areas (customer care and billing, provisioning and order processing, and network operations management), and compliance to TMN layers, such as business, service, network, and element management layers.

Intranets are penetrating both the telecommunications providers and enterprise infrastructures. This contribution targets the management of these kinds of networks. In detail, it identifies sensitive components that may cause congestion or bottlenecks. Special emphasis is on log file analysis, wire monitoring, look-through measurements, traffic shapers to conserve bandwidth, and on administering Web server farms. For each subject area, product examples are also included. In most cases, Web content is expected to drive decisions about resource facilities and equipment reservation/allocation.

3.1 Management Concepts

Joe Ghetie

The last decade of the past millennium witnessed one of the most dramatic advancements of communications technologies and services in human history. Communication, as a way of conveying and exchanging management information, had found in the Internet one of the best examples of the explosive growth with a tremendous impact on the current and future abilities of humans to share information.

The dream of universal access to information, the dream of a giant village, the dream of fast, reliable, content-rich information exchange are today closer to reality than anybody has anticipated. Data communications, video communications, and both wired and wireless communications media have increased our ability to control through communications large, global enterprises and businesses.

Network and systems management are specialized systems targeting, monitoring, and controlling the vast array of network and computing systems resources used in communications, manufacturing, commerce, finance, banking, and education, as well as in research and development.

Management systems were born out of necessity to prevent, diagnose, configure, and solve problems raised by the size, complexity, and heterogeneity of multivendor, multiprotocol, and multitechnology environments that characterize the underlying network and computing systems.

Although management systems are value-added components to communications technologies, they are as vital as the transmission, switching, and operations systems in order to supervise and maintain the normal information exchange.

3.1.1 Management and Data Communications

Management systems aimed at monitoring and controlling communications systems represent conceptual design and associated infrastructure that, essentially, resemble particular implementation of open systems.

3.1.1.1 Communications General Model

A simplified view of any point-to-point communication assumes an information source (sending party) and the information destination (receiving party). The communication takes place over a transmission

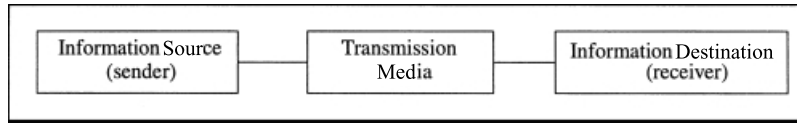

FIGURE 3.1.1 Communication network conceptual model.

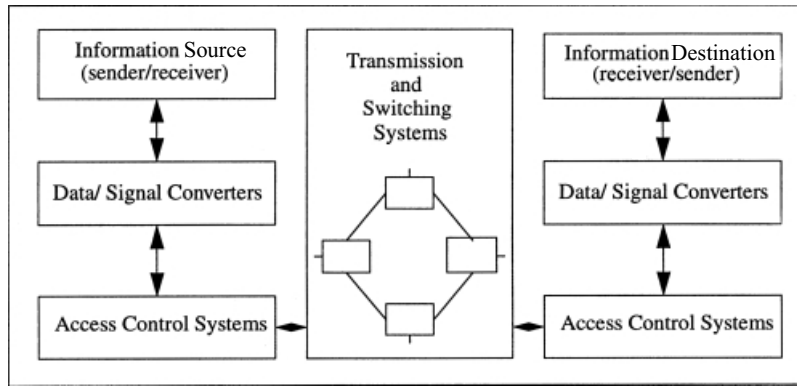

FIGURE 3.1.2 Communication network conceptual model.

media which can be a pair of copper wires, coaxial cable, fiber optic, or a wireless media such as radio, microwave, satellite, or infrared rays (Figure 3.1.1).

The information source can be a telephone set, a computer, a TV pattern, a facsimile, or an instrumentation process. The information can be another telephone set or a computer, a TV set, a fax machine, or a control panel.

In order to be transmitted, the native information sources, voice, computer or instrumentation data, graphics, or video images require successive data/signal conversions, according to adopted communications media and transmission technologies, and a rigorous security control of the access to shared network resources. Therefore, new components such as data/signal converters and access control systems should be added to the communication model. This communication can be asymmetric, i.e., taking place only in one direction, or it can be symmetric, i.e., taking place bidirectionally (Figure 3.1.2).

As a further consideration, the box representing the transmission media becomes more than a single conduit; a mixture of transmission/transport components and switching components in the form of circuits, links, nodes, routers, and switches participates in the design of a shared network environment.

3.1.1.2 Network Management General Model

The task of management, as derived from the general model of communications, is very clear: to be able to supervise, monitor, and control all the components that participate in the process of communications from the source to destination. That might include various computer hosts and terminals as sources/destinations of information, the devices performing data/signal conversions (protocol converters, emulators, concentrators, multiplexers), devices required to control the access to the network (security access, authorization, encoding, encryption), and all the components used in transmission, switching, and routing (Figure 3.1.3).

The task is not only clear but quite challenging when the list of actual devices is spelled out. Many dozens of different technologies implemented in hundreds of different components, developed, designed, and manufactured by thousands of vendors, are all potential subjects of management systems, especially when it comes to the point of providing end-to-end, enterprise-wide management services from monitoring, diagnostics, control, and reporting.

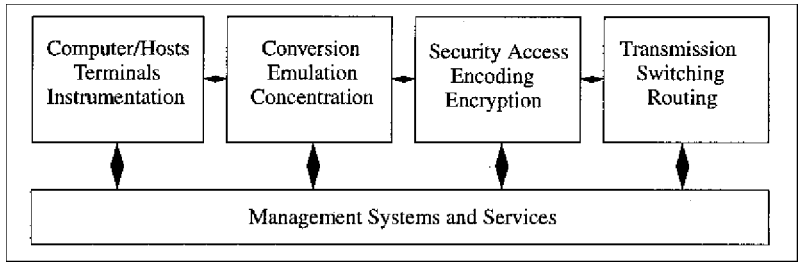

FIGURE 3.1.3 Network management conceptual model.

PCs, workstations, minicomputers, servers, mainframe computers, terminals, test equipment, phones, PBXs, TV sets, set-top boxes, cameras, modems, multiplexers, protocol converters, CSU/DSUs, statistical multiplexers, packet assembler dissassemblers, ISDN adapters, NIC cards, codecs, data encoders, data compression devices, gateways, front-end processors, line trunks, repeaters, regenerators, matrix switches, DCS/DACs, bridges, routers, and switches just begin a list of devices which should be or might be managed.

The management picture is complete only if we consider, in addition to the management of network resources, the management of computing systems resources such as thousands of different businesses, users, systems applications, databases, and complex, specialized, large operations systems.

All the information collected and exchanged in conjunction with management operations is translated in management data which is manipulated using techniques similar to those employed by data communications networks. However, substantial differences exist between data communication exchange and management information exchange to claim a specialized technical field, specialized communication protocols, information models, and specialized skills to design and operate management systems and interpret fault, performance, configuration, or security management information.

The following subsections will explain what is peculiar in management systems, the major requirements appended to management systems, the management paradigms adopted in management, and the historic and technical evolution of management systems.

3.1.2 Management Requirements

The diversity of managed resources, as found in traditionally distinct fields of communication such as voice, data, and video communications, generate different views on what should be the management functions and management requirements associated with management systems.

3.1.2.1 High-level Management Functions

Regardless of the diverse management views, three high-level management functions top the list: **monitoring**, **controlling**, and **reporting**. Monitoring represents the continuous collection of management information about the status of management resources, delivered in the form of events and alarm notifications when the threshold attached to managed resource parameters is exceeded. Controlling is the targeted attempt of the manager or management application to change the status or configuration of selected managed resources. Reporting consists of delivering and displaying the management information in an accessible form for reading, viewing, searching, and ultimately interpreting the reported information.

In practice, several other functions are associated with management systems and management applications according to particular business needs such as provisioning, service activation, capacity planning, network/systems administration, inventory management, backup and recovery management, and management operations automation. Many of these complex functions include or are built on basic monitoring, controlling, and reporting.

3.1.2.2 High-level Users Management Requirements

Based on the users' perspective on management, we can derive a set of high-level requirements associated with management, as listed below:

a. Ability to monitor and control end-to-end network and computing systems components.
b. Remote access and configuration of managed resources.
c. Ease of installation, operation, and maintenance of the management systems and their applications.
d. Secure management operations, user access, and secure transfer of management information.
e. Ability to report meaningful management-related information.
f. Real-time management and automation of routine management operations.
g. Flexibility regarding systems expansion and ability to accommodate various technologies.
h. Ability to backup and restore management information.

3.1.2.3 Driving Forces behind Management Technologies

Although the term of "network management" gained a clear acceptance only in the mid 1980s with the advancement of IBM management tools (later incorporated into the IBM NetView family of management products), network management was equally driven by the development of telecommunications, data communications, and computing systems networking. For telecommunications and data communications, the management technologies were concentrate on management of transmission and switching equipment (hardware devices, connections, circuits) along with conversion and access control devices. In the case of computing systems, the management technologies were concentrate on managing large computing system resources (hardware, interfaces, memory, data storage devices, etc.) and applications/databases.

With the convergence of telecommunications and computing systems, which embraces various technologies commonly known as computer telephony integration (voice over Internet is one of the most recent developments), the common point of these major fields becomes the network which connects these systems and the management of large data communications networks. This will be the dominant factor of the networks of the future.

3.1.2.4 Justifying Network Management Investment

It is well known that management systems are perceived as overhead cost. However, the cost of not being able to prevent major network and systems problems or to quickly find and restore a system to normal functionality is even higher and can be crippling for many businesses relying on information exchange.

The following reasoning can be used in justifying the investment in network management. Some points can be quantified and used as a basis for a front-end analysis when selecting management systems.

a. Reducing downtime of critical components of networks and computing systems.
b. Controlling the corporate networks as strategic investment assets.
c. Controlling the performance, growth, and complexity of user application.
d. Improving services in customer support and security of data transfer.
e. Controlling the cost of information technology deployment and operations.

3.1.3 Management Paradigms

Before analyzing the capabilities or the openness expected from management systems, we have to understand the fundamental paradigms used in management and the views associated with these paradigms.

3.1.3.1 Management Basic Model

Conceptually, the management systems are based on a simple model. In this model, management is the interaction/cooperation between two entities: the **managing entity** and the **managed entity**. The management entity represents a management system, a management platform, and/or a management application. The managed entity represents the managed resources. Looking at this simple model, it is

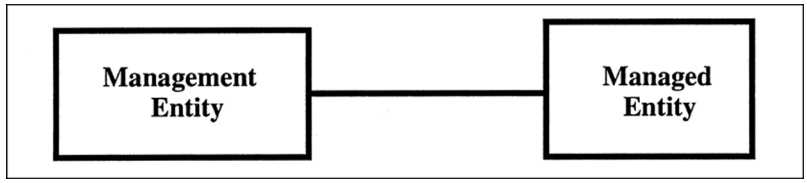

FIGURE 3.1.4 Management basic model.

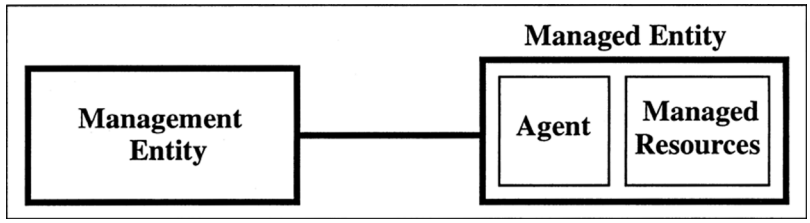

FIGURE 3.1.5 Manager-agent model.

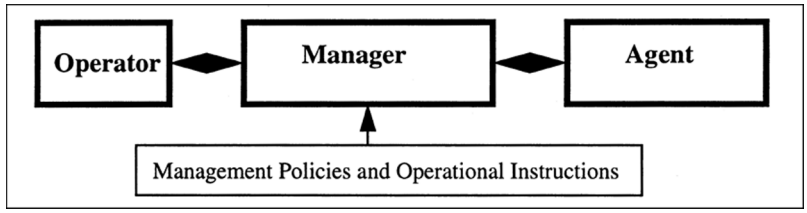

FIGURE 3.1.6 Real manager-agent model.

important to note its similarity to the basic communication model presented at the beginning of this chapter (Figure 3.1.4).

In order to communicate with the managed resources, which do not have any native mechanism to pass management information, there is a need to create an intermediary component, the agent. The agent is also called management agent or managed agent. The manager is the management entity, while the agent hides the interaction between the manager and the actual managed resources (Figure 3.1.5).

The manager–agent model is very common, used in describing the interaction between the management entity and the managed entity at a high level. This is the reason that all the paradigms natively created for management purposes closely follow the manager–agent model. In reality, the manager–agent model is more complex (Figure 3.1.6).

The complexity becomes more evident when we consider the interactions between the manager or the management applications and the human operators. Other components, less visible but also very important because they shape the nature of interactions between managers and agents, are the **management policies** and the **operational instructions** given to the manager and implicitly to the operator.

There are other paradigms such as client–server and applications–object server that can be used for management information exchange. Natively, these paradigms have been conceived for building distributed applications or distributed object environments. Nevertheless, these general paradigms can be applied for management and there are products that use variations of these paradigms for management purposes.

3.1.3.2 Management Views and Associated Models

Management assumes, as a primary function, the communication between the managing entity and managed entity. The management communication is based on the request–reply paradigm. The manager

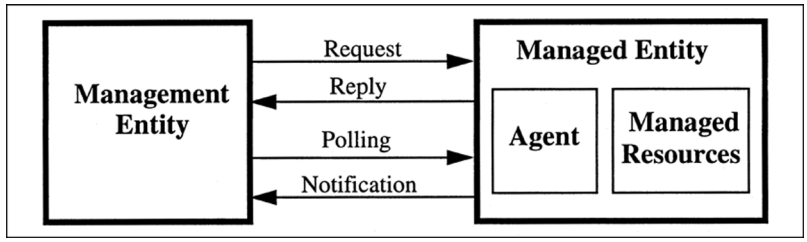

FIGURE 3.1.7 Manager-agent communication model.

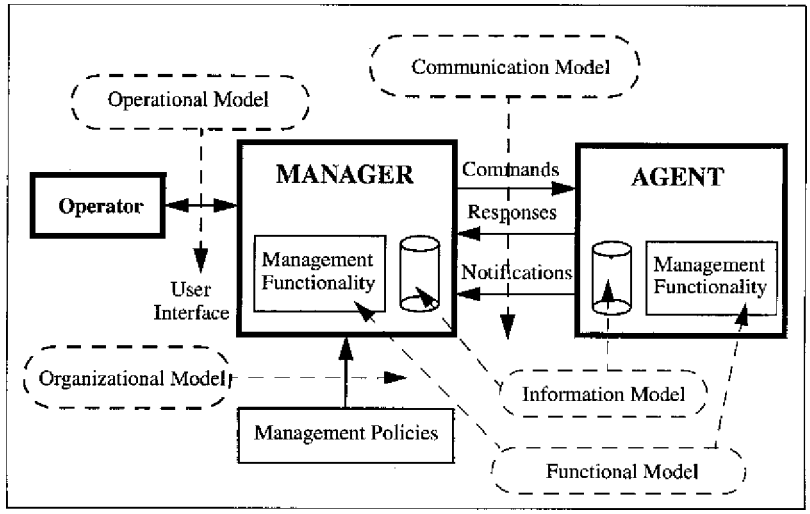

FIGURE 3.1.8 Manager-agent relationship models.

will request from the agent specific management information and the managed entity, through the agent, will reply with a message containing the information requested. If the request–reply communication is used continuously in order to reach each agent and the corresponding managed objects, the mechanism is called polling and it is primarily used in the management of Internet environments based on the Simple Network Management Protocol (SNMP) (Figure 3.1.7).

The request–reply mechanism is considered a synchronous communication mechanism, i.e., the manager expects an answer from the agent in a limited time frame before taking any action. If the reply is not received, a request for retransmission should be initiated by the manager.

There is an additional mechanism for communication between the manager and agents, called notification. The notification is an asynchronous mechanism initiated by the agent that communicates to the manager important changes in the status of managed resources which require either manager attention or intervention.

When building management systems, there are many aspects that should be taken into consideration. In addition to the communication model, several other models are used in conjunction with the manager–agents relationship, as follows: architectural model, organizational model, functional model, and informational model (Figure 3.1.8).

The architectural model deals with the design and structure of the components participating in the management process, i.e., the manager or managers and the agents supplying management information according to the network topology. The manager can be designed as a management platform that consists of a management framework and a suite of management applications providing the actual management functionality such as configuration, fault, and performance management. More details will be provided in the sections dealing with management platforms.

The operational model deals with the operator's interface to the management system and specifies the nature and the type of interactions available to the user such as controlling managed objects, displaying and searching for specific events, dialog with the systems, and alerting the operator in case of critical alarms. Most of the operational specifications are included in the product's technical specifications such as user guide, administrative guide, etc.

The functional model refers to the structure of management functions performed by the management system through management applications. The functional model is considered a layered model where basic management functions such as configuration, fault, performance, security, and accounting management are the foundation of the functional model. Several other management functions such as trouble ticket administration, help desk, provisioning/service activation, and capacity planning consist of a combination of the basic management functions. At the pinnacle of the functional model, there are applications performing complex functions such as alarms/events correlation, expert systems, and management automation.

The organizational model is tightly linked to the overall management policies and operational procedures. This model specifies management domains, partition of management realm among the management operators, access of the user to the management systems, customer-based network management, interchangeability of the roles between managers and agents, and the overall cooperation between the manager and other managers or management applications.

The information model, although mentioned at the end of this list, is critical in handling all the management aspects. Given the variety of managed resources, in order to support their management in a common way, there is a need of an abstraction of managed resources in the form of a common information model, known by both manager and agents. The management information model establishes the basis for defining, naming, and registering the managed resources. Managed objects are considered abstractions of physical and logical managed resources. Therefore, the term of managed objects implies the use of an information model. Access to the managed resources is allowed only through the use of managed objects. The conceptual repository of management information is called management information base (MIB). When we refer to a particular MIB, that means a collection of managed object definitions that describe a particular management domain or environment. The definition of managed objects is standardized and on this basis a manager implementing a particular protocol and information model can communicate with distributed agents which implement the same MIB.

3.1.3.3 Management Domains

Historically, as we mentioned earlier, the notion of network management was launched by IBM. The IBM NetView products were in fact a combination between mainframe systems management and network management. Since then, the concept of management has evolved. At the beginning, the management products have reflected the division, typical to most of the businesses, between network and computing systems management. With the advent of management platforms, the difference between network and systems management is blurring since the nature of the application and not the platform framework will determine the use of management systems.

Currently, it is commonly accepted that two major management domains can be considered when discussing the nature of managed resources: managing **physical resources** and **logical resources**. Physical resources are considered all the hardware components of the telecommunications and data communications networks that participate in the process of exchanging information. This management domain is known as **network management**. The management of computing systems' physical resources such as processors, memory, input/output interfaces, and storage devices, are considered part of systems management.

The management of logical resources is built around **applications management** and **databases management**, both associated with computing systems. Service management, user management, management of distributed transaction services, and data flow management are also considered system management of logical resources (Figure 3.1.9).

There is a separate domain which deals with the management of specific logical resources, i.e., the protocols used in standards-based communications. Layered protocols, layered service primitives, and

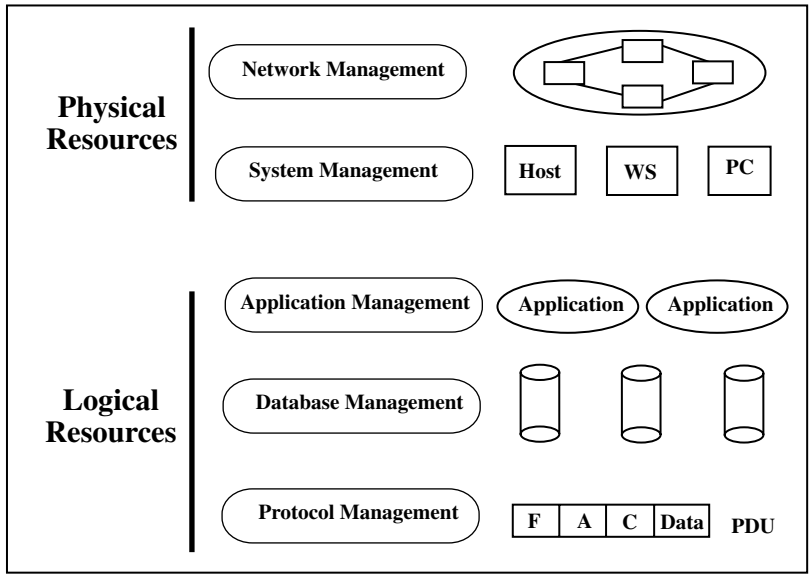

FIGURE 3.1.9 Management domains classification.

embedded management services are examples of protocol management. This type of management is applied to interfaces of particular technologies such as ATM, SONET, and WDM in the form of embedded channels or embedded **layer management entities** (LMEs). This type of management is conceptualized in the OSI Basic Reference Model, the foundation of standardized layered architecture and management.

3.1.4 Open Management Systems

In order to evaluate the management systems, there is a need for a reference model. This reference model is the open system and its corresponding model, the open management system.

3.1.4.1 Open Systems Conceptual Model

The open systems conceptual model assumes a design of systems modeled by the presence of four entities and by the relationship between these entities: **application platform, applications**, **application programming interface** (APIs), and **platform external interface** (PEI). This model can be applied to any computing system as part of the overall design and implementation. What makes any computing system (which runs software programs or applications) an open system is the separation of applications from the applications platform through APIs (Figure 3.1.10).

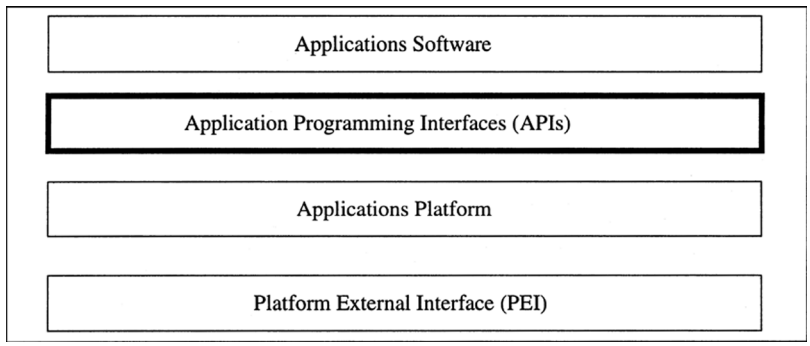

FIGURE 3.1.10 Open systems conceptual model.

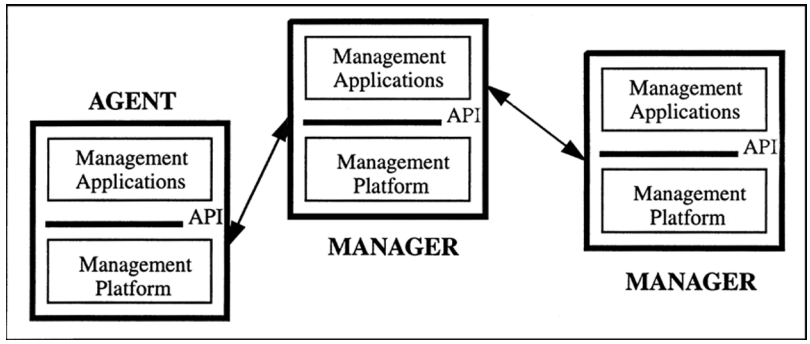

FIGURE 3.1.11 Open management system.

3.1.4.2 Open Management Systems Concept

The open systems conceptual model can also be applied to management systems, i.e., to managers and managed agents. In this case, the applications will be specialized management applications providing fault, configuration, performance, security, and accounting management. The management platform is a management framework which consists of, in addition to the computing platform, specific management services such as event management services, communication services, graphical user interface services, or database services (Figure 3.1.11).

As mentioned earlier, key components to open systems are the APIs. In this case, the APIs are specific management APIs that allow the development of management applications by using specific management platform services. Last but not least, the management platforms are not isolated; they communicate with managed agents (as a minimum) or with other management systems which may be modeled as open management systems. The platform external interface, in this case, will be an open standardized interface with well defined management operations, services, and protocols.

3.1.4.3 Requirements for Open Management Systems

Four high-level requirements characterize open systems and open management systems: **operability**, **interoperability**, **portability**, and **scalabilty** (Figure 3.1.12).

Operability represents the ability of management systems to provide easy installation, operations, and maintenance, as well as adequate reliability and performance. Interoperability represents the ability of management platforms to transparently exchange management information with managed agents or peers' management systems. Portability expresses the ability of management platforms and/or management systems applications to be ported to a different environment (computing platform) with minimum changes or no changes. Scalabilty refers to the ability of management systems to be expanded in coverage, user domain, and management functions without the need to change the initial design.

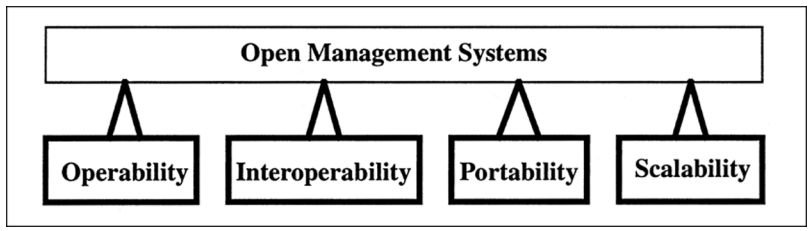

FIGURE 3.1.12 Open management system major requirements.

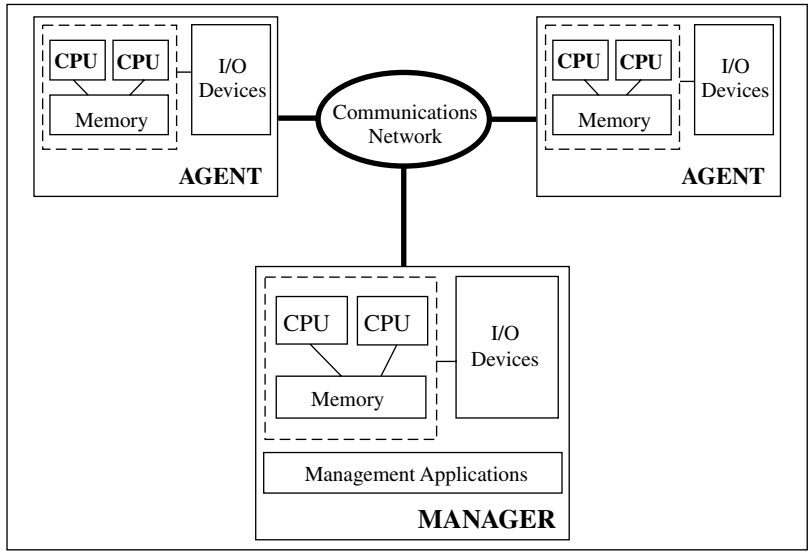

FIGURE 3.1.13 Management of distributed systems.

3.1.5 Distributed Management Systems

Most of the computing systems, telecommunications, and data communications networks are distributed, i.e., interconnected by a communication network designed to transfer information and messages related to specific business needs. Management means managing various network and systems resources which in most instances are physically separated. Therefore, by its very nature, the management is distributed.

A system is considered autonomous (it can be simple processor or multiple processor based) if the processes that constitute the system share the same memory. In contrast, distributed systems consist of interconnected autonomous systems with no shared memory. Since any networked computing environment is inherently a distributed system, the management of these systems is also inherently distributed.

3.1.5.1 Distributed Network and Computing Systems

The true nature of management, as distributed or centralized, is determined not by the physical distribution of its components (managers and agents) but by the centralization and processing of management information (Figure 3.1.13).

If the system is designed to collect all the management information from all the agents (which constitute the management domain) in one point, we deal with a centralized type of management. If the collection of management information takes place in several interconnected processes and the information may be held in distributed databases, we deal with distributed management systems.

3.1.5.2 Distributed Management Systems Architectures

In a truly distributed management system, multiple management users or operators as management clients access the management server through a local or a wide area network. The actual manager runs the management applications and it is the holder of a MIB for a particular management domain. Each manager is responsible for the agents that are part of his/her domain.

The ability to exchange management information between servers (managers), keep in synchronization the shared MIB information, take over the management domain of a failed manager, and of the operators to interact with multiple managers, creates a truly distributed management system architecture (Figure 3.1.14).

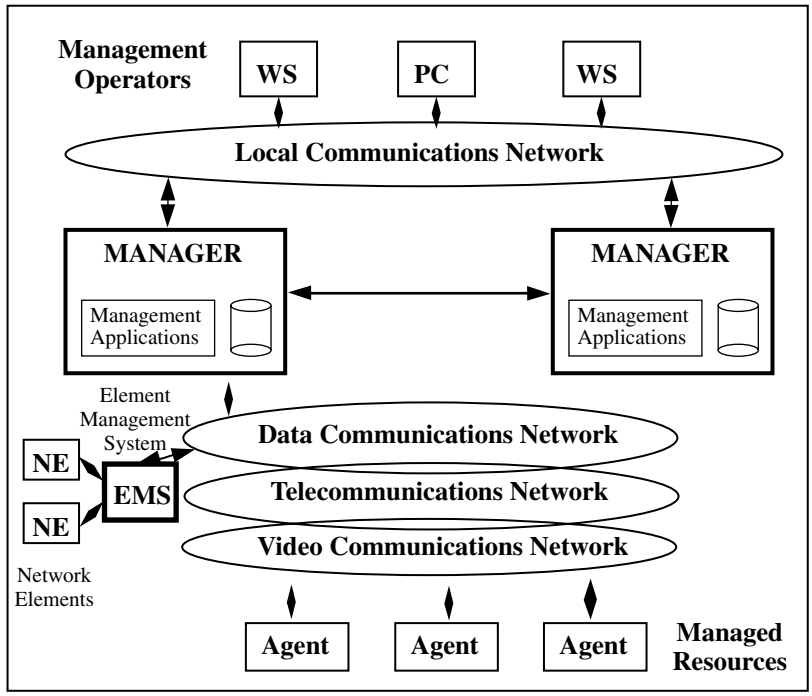

FIGURE 3.1.14 Distributed management systems architecture.

We have to emphasize that in all these examples we assume that the manager has a high degree of remotely accessing and configuring agents, with each agent acting as a management agent for a collection of managed objects and management processes.

3.1.5.3 In-band and Out-of-band Management Systems

All of the diagrams were presented in order to introduce the management concepts, and the properties of the management field included representation of interconnecting networks that carry management information. It is important to emphasize that these networks have rarely been designed as management-only infrastructures. Most of the management systems use for management information exchange the very network that carries the business-related data, voice, or video information. For the purpose of management, specialized protocols, operations, and application entities have been created and used. However, the management information is carried on the same physical infrastructure and on the same communication stack as the business information. In this case, we deal with the **in-band** type of management. This is a very cost-effective solution. However, there are some issues. By sharing the same service channels, the management information may take a significant chunk of the available bandwidth, and this may affect the overall performance of data exchange. That puts restrictions on how much and how often information is collected.

This is the reason that some management systems are built using **out-of-band channels**. The out-of-band management solutions may include unused bandwidth from a current channel allocation. A good example is the use of the low-band portion (50Hz–200Hz) of the voice grade channels as a dedicated data channel for management purposes. This solution is used for the management of the modems that share the same infrastructure with the voice communications. Other solutions consist of reserving a bit from the normal bit stream (for example, T1 multiplexer) to create a dedicated data channel for management purposes or assigning fields in each of the transmitted frames or cells for management purposes as it happens in the SONET and WDM technologies.

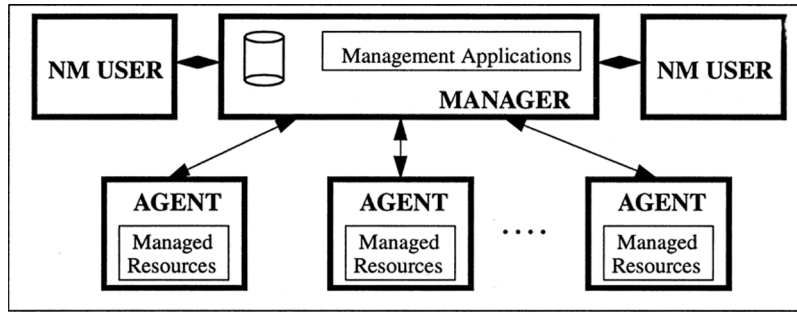

FIGURE 3.1.15 The "single manager" topological framework.

3.1.6 Management Systems Topological Frameworks

At a very high level, the architectural model of management systems is understood as the relationship between the main components of management systems, the managers and agents. The accepted term for the architectural layout of the management network is called topology and in most cases follows the business network infrastructure.

The topological view is the basis for the representation of the network and systems components using graphical user interfaces. An elaborate collection of graphical icons representing logical and physical resources, the links between these icons and the colors associated with the status of managed resources allow the management operators or the users to have a view of the management components along with their status.

Three major topological frameworks are considered when designing management systems: **single manager**, **manager of managers**, and **network of managers**.

3.1.6.1 The Single Manager

The single manager topology framework uses one management system which concentrates the collection and processing of management information from various managed resources such as routers, bridges, multiplexers, matrix switches, etc. Thus, the manager is the only point of exercising control over the network.

The system playing the role of the manager is usually a monolithic application that performs management operations and stores the management information received from all the managed resources. The single manager topology is fully centralized. Historically, most of the management systems started as host-based, centralized systems. Today, they still represent the most common topological framework (Figure 3.1.15).

Regarding the single manager framework, we emphasize its weaknesses as follows: concentration of network management functions and applications in one point; limitation of the number of resources to be managed (lack of scalability); and the high vulnerability of these systems when the manager fails. This topological framework is used for the management of small- to medium-size networks and systems.

3.1.6.2 The Manager of Managers

The manager of managers (MOM) topology is a logically centralized framework with distributed control capabilities. The MOM acts as a single integration point for several distributed element management systems (EMSs) (Figure 3.1.16).

The actual management of managed resources/devices is provided by the EMSs that monitor and control a particular management domain, which may consist of a group of network components and associated applications. Usually, EMSs are designed to manage a family of similar products built around a particular technology. In other instances the management domain is determined by geographical, administrative, or jurisdictional considerations.

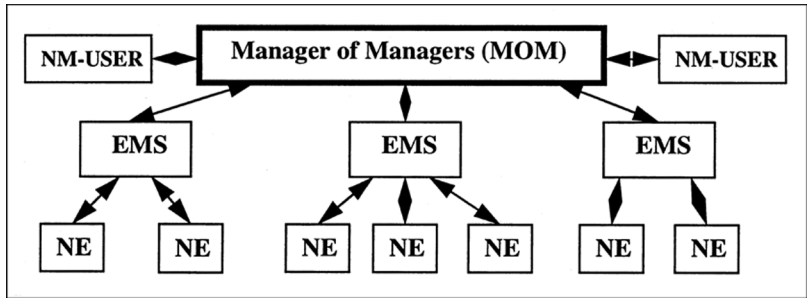

FIGURE 3.1.16 The "manager of managers" topological framework.

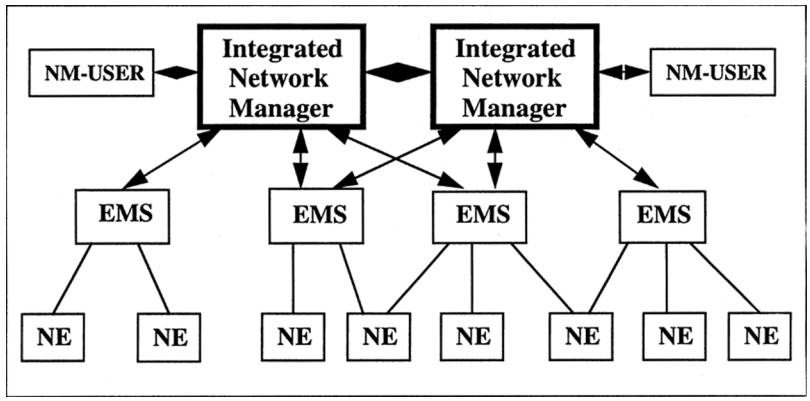

FIGURE 3.1.17 The "network of managers" topological framework.

This topology is used for medium and large networks. Only vital, critical information such as alarms, security alerts, and capacity planning-related information is elevated to the level of MOM, which acts as a management integrator.

3.1.6.3 The Network of Managers

The network of managers topological framework provides fully distributed management based on cooperative management between integrated network managers (INMs).

In this topological framework, management information can be exchanged between peer managers. Each INM is responsible for the management of its own grand domain. Cooperative links between INMs allow management information exchange. More than that, each INM can take over the management functions of an adjacent manager. Within each domain, the INM acts as the focal point of distributed management provided by several EMSs (Figure 3.1.17).

3.1.6.4 The Management Platforms

Management platforms do not represent a new topological framework; thus, they can be used in any of the topologies described in this section. The management platforms are designed as open management systems to allow the development and operation of portable distributed management applications. By employing, as part of the platform framework, advanced management services such as directory, security, and time services, in addition to basic communication, event management, graphical user interface, and database services, the management platforms can manage large, heterogeneous, multivendor, multitechnology, and multiprotocol environments.

Several management platform components such as graphical user interfaces, management databases, and management applications can be distributed among several computing platforms. Multiple management

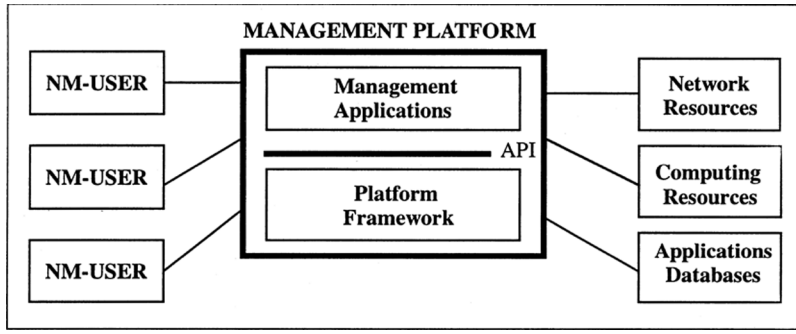

FIGURE 3.1.18 Management platform framework.

platforms can communicate to each other in order to manage large administrative domains (Figure 3.1.18).

3.1.7 Management Systems Evolution

Although the management systems have been established as specialized systems to manage large and complex network and computing systems since the mid 1980s, distinct events and distinct phases can be identified in the technical and chronological evolution of management systems.

3.1.7.1 Management Systems Technical Evolution

The first phase in the management systems development is exemplified by **passive monitoring systems** targeted solely toward network components management and providing test, instrumentation, and protocol analysis results. This was characteristic for the management systems designed in the late 1970s and early 1980s.

The next major phase was the build-up of **element management systems** (EMSs) which provide monitoring and controlling capabilities of individual systems. Acting as stand-alone systems, the EMSs target the management families of network elements, equipment, and hosts. Generally, the EMSs contain a single management application bundled with the computing platform, forming the actual run-time operational management environment. These types of management systems were typical in the 1980s and they covered the management of modems, multiplexers, T1 multiplexers, matrix switches, etc. In most cases, the management was limited to one type of equipment provided by a single vendor (Figure 3.1.19).

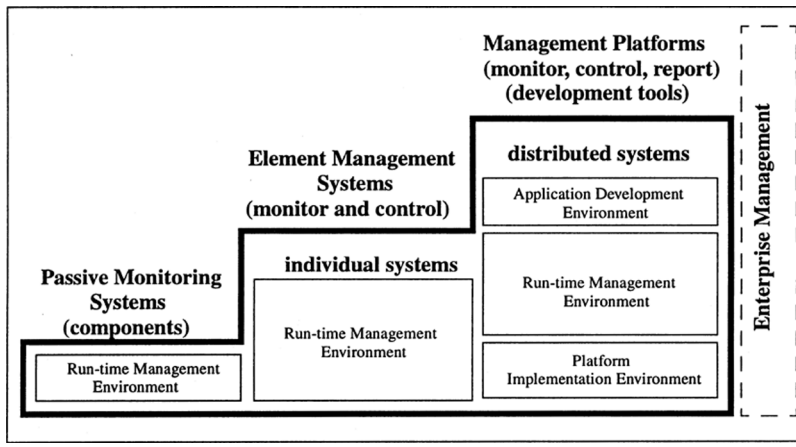

FIGURE 3.1.19 Management systems evolution.

Management platforms are the third major generation in the history of management systems development that go beyond the run-time operational environment which characterized the earlier stages. By adding an application development environment with tools and APIs which allow multiple and portable applications to run on top of management platform framework, the management platforms have embraced many of the concepts of distributed open management systems.

The run-time environment is represented by common management services provided by the platform and reflects the overall operability aspects of a management platform. The development environment includes the run-time environment and provides portability for management applications and integration of these management applications with the platform services. In order to develop management applications that use platform management services, the development environment should include the run-time environment. In addition, the complexity of management platforms requires an implementation environment for testing and conformance to standards or vendor specifications. The implementation environment provides means to assess the management platforms' interoperability. More details about management platforms will be provided in the following two sections.

3.1.7.2 Management Systems Chronological Events

In order to fully understand the evolution of management systems, it is very important to provide a more detailed, chronological order of all the events that ultimately shaped the field of management. It is well known that, traditionally, management systems trail the development of new network or computing technologies. In many instances, management solutions are afterthoughts, ad-hoc, and patched solutions. That creates later problems because the management is modeled, designed, and processed in systems outside of the technologies that are managed. The technical design and the economies of a later-added management are always inferior to the one delivered as part of the native technology. This is a major shortcoming of overall network and computing systems management and it will very likely persist in a wild competitive environment where the designers and manufacturers of new technologies continue to rush their products to market even though the management of that technology is missing or is not mature enough. This situation explains the existing differences in achieving standardization for network and computing systems management.

The following list of events, in chronological order, attempts to capture the evolution of management systems.

IBM mainframe-based data extraction and performance analysis tools, 1980–1985
IBM NetView, and integrated systems and network management, 1986
AT&T Unified Network Management Architecture (UNMA), 1987
DEC, Enterprise Management Architecture (EMA), 1987
Element Management Systems (EMSs) from Timeplex, Paradyne, Codex, GDC, 1987-1989
OSI Management International Standardization (starting in 1989)
Network management platform concept advanced by DEC, HP, IBM, OSF, 1989
Adoption of graphical user interface for network/systems topological display, 1990
Internet SNMP-based recommended standards adoption, 1990
OSF Distributed Management Environment (DME) proposal and subsequent RFPs, 1990
SUN SunNet Manager, Unix-based workstation management solution, 1990
OSF DME technology candidates selection, 1991
ITU-T, ANSI T1M1, ETSI contribution toward TMN interface standardization, 1992
Commercial management platforms, HP OpenView, Digital DECmcc, Tivoli TME, 1992
IBM SystemView blueprint and SystemsView for AIX platform, 1993
Home-grown management platforms from NetLabs, Cabletron, OSI, 1994
OSF DME delivered as the network management option (NMO), a major failure, 1994
HP OperationsCenter and HP AdministrationCenter systems management platforms, 1994
NM Forum, SPIRIT management platform requirements, version 1, 1995
DSET provides stand-alone management applications and agent development tools, 1995

Tivoli Systems TME acquired by IBM, integration plan with SystemsView for AIX, 1996
AT&T OneVision management platform-based integration solutions is proposed, 1996
HP OpenView DM 4.x, advanced distributed management versions, 1996-1997
Computer Associates Unicenter TNG management platforms, 1997
SUN Solstice Enterprise Manager platform and family of products, 1997

By the end of 1997 most of the surviving management platforms had become mature products although they were still far from the ideals of fully open, distributed management platforms. Evidently, the biggest failure was the standardization of management platform framework, as a collection of interchangeable management services. Few management platforms are designed and built according to the advanced features of object-oriented information modeling.

With all of these shortcomings the management platforms are the best hope to build enterprise-wide management systems where integration of management solutions and scalability are two major issues.

3.1.7.3 Management Platforms for Enterprise-wide Management

In the previous sections we indicated the complexity and difficulties confronting the management field. We also indicated the shortcomings in the historical development of management systems. Management platforms do not solve these shortcomings overnight but they bring a flexible approach to the management of multivendor, multitechnology, multiprotocol networks and systems environments. This is why a close look at the design of management platforms is necessary.

Management platforms, either as autonomous or interworking management systems, should provide several basic management functions. First of all, a management platform has to communicate with the external world through platform external interfaces, i.e., it has to provide communications services. Next, management information is exchanged in the form of management events that have to be stored, processed, and named. Therefore, there is a need for event management services. Furthermore, the events, as related to the management of network or computing systems resources, should be displayed (after the necessary processing) by using graphical user interfaces. Management information and all the components associated with management are organized using managed object models. Therefore, there is a need for a service that provides manipulation of managed objects. Ultimately, the management information about network configurations and managed resource status and parameters has to be stored in databases. Such database service may allow near real-time presentation of the status of the managed systems and components. Additional management operation services are needed to support all of the other platform services. In addition to these management services, there is a need for other distributed management services such as time service (synchronization), directory service (naming), and security services (Figure 3.1.20).

User interface services provide support for presentation of management information and support for interactions between users/human operators and distributed management applications used to manage network and computing systems. These services support both graphical user interfaces (GUIs) and asynchronous command line interfaces, by providing network and computing systems layout display based on visual icons, windows environment manipulation, on-line information, and general support for common applications development. The user interface is the most visible point of integration between various platform components and management applications.

Event management services provide common services to other platform management services and to the management applications running on top of management platforms. The events can be generated by network/computing systems, components state changes, systems errors, applications, and by users/operators. Common event operations include event collection, event logging, event filtering, and event administration.

Management communications services, either object-based or message-based, provide support for communications interfaces, management protocols, and communications stacks used to carry management information. Primarily, this support targets standardized management protocols such as Simple Network Management Protocol (SNMP), Common Management Information Protocol (CMIP) and Services (CMIS), and Remote Procedure Calls (RPCs).

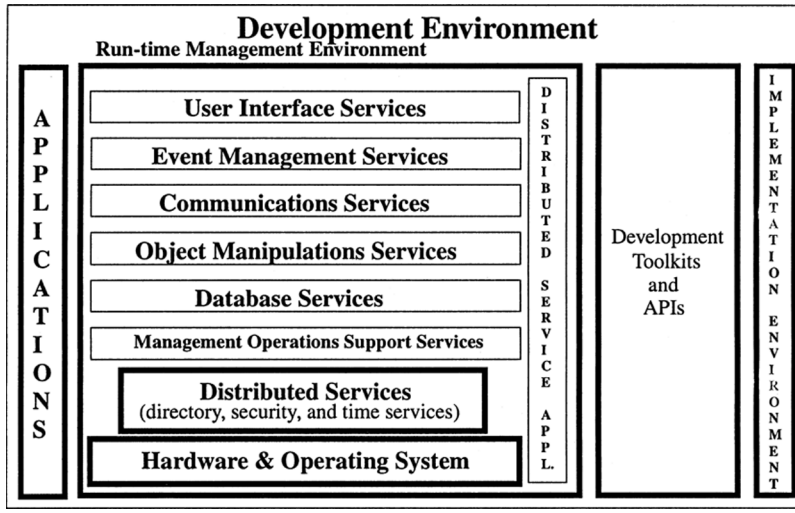

FIGURE 3.1.20 Management platform architectural components.

Object manipulation services provide support for information exchange between objects as abstractions of physical and logical resources ranging from network devices and computing systems resources to applications and management services. Primarily, this support targets object interfaces as defined by the OMG Common Object Request Broker Architecture (CORBA) and OMG Interface Definition Language (IDL). Object manipulation includes operations on the MIB, object support services providing location transparency for objects exchanging requests and responses, persistent storage for MIBs, and support for object-oriented applications development.

Database services provide support for management data storage and retrieval along with its integration with various platform services and management applications. Management information can include dynamic instance information related to configuration events, fault events, or performance events, to historical and archive information for security audit trail. The database services include database management systems (DBMSs), standardized database access and retrieval mechanisms such as structured query language (SQL), database concurrence mechanisms, and data backup mechanisms.

Management operations support provides common services to the management platform core and to the management applications running on top of the platforms. It includes management of the background processes associated with the platform hardware and operating system, and the handling of management applications.

Regarding management applications running on top of the management platforms, they can be classified in two major groups: core management applications and resource-specific applications. Core applications include functional management applications to manage specific management functional areas (SMFAs) such as configuration, fault, performance, security, and accounting management. Core applications also include compound applications which provide cross-area functionalities, as required by user needs and business considerations (e.g., trouble ticketing). Resource-specific applications, as the name indicates, are built specifically to manage particular network devices or computing system components.

The management applications development environment mirrors the run-time environment and includes specific development tools for user interfaces, event management, communications, object manipulation, and database operations. The APIs for various platform management services are critical components in the development environment. The development environment includes the run-time environment since the newly developed management applications are tested against the run-time environment.

The management implementation environment mainly refers to the overall acceptance testing of management platforms as they are used in the management of real network and computing systems. Implementation testing is different from the testing done on various platform hardware and software

components during their development and production. The implementation environment covers effective systems testing based on test criteria, test procedures, and test tools used to operate, maintain, and troubleshoot complex distributed systems, which are tailored to management platforms.

As we mentioned earlier, the management platform consists of management services and the actual management applications that run on top of management services. Both management services and management applications make use of the computing hardware and operating system. Although the design of the hardware and operating system is outside the scope of management platform design, it is important to understand the differences between various computing systems and to understand the alternatives in selecting hardware and operating systems. In a truly open system environment, the platform services and applications are supposed to be hardware and operating system independent.

3.2 Management of Emerged and Emerging Technologies

Kornel Terplan

3.2.1 Introduction

Telecommunications services offered by domestic and international providers are based on a mixture of emerged and emerging technologies. Emerged technologies include private leased lines on T/E-basis, ISDN, traditional voice networks, message switching, packet switching, and SS7-based signalling. Emerging technologies are the following: frame relay, FDDI, ATM, SDH/Sonet, SMDS, wireless, cable, and xDSL.

Due to rapid progress made in technologies and infrastructures, the number of choices to offer certain telecommunications services is continuously increasing. In layered communications structures, technology usually occupies the lower layers. It is true for both TMN and OSI layers. If IP-based services are the goal, this service can be deployed in various ways. The supporting lower-layer infrastructure is going to be reassessed. Besides the traditional IP-ATM-Sonet/SDH combination, other options are also under consideration. This alternative is conservative, less risky from the engineering point of view, and achievable now. It may, however, lead to low efficiency and to high costs. Enhanced frame relay may substitute ATM everywhere, offering lower costs at good quality of service (QoS). But, in certain areas, there are no QoS standards available. ATM transport may eliminate the Sonet/SDH-layer offering ATM ring functions similar to distributed ATM switches. There are just a few vendors who consider this option. ATM/IP hybrids on the basis of Sonet/SDH would reduce the number of routers, with the result of lower management expenses. This technology is in the test phase, still unproven. IP over Sonet/SDH eliminates the ATM layer completely. If megarouters are at cost parity with ATM switches, this alternative would be the low-cost IP delivery solution. This technology is unproven; operating costs of megarouters are difficult to predict. Optical IP would be the lowest cost delivery of IP services. In this case, IP is directly connected to the optical subnetwork of Layer 1, neither using ATM nor Sonet/SDH. It is the least proven technology; there are serious concerns about fault management with this alternative.

This contribution investigates the manageability of both emerged and emerging technologies. Each technology discussed will be introduced briefly without details. Emphasis is on the availability of management information bases (MIBs), management protocols used, and management products usually deployed.

3.2.2 Foundation Concepts for Networking Technologies

The majority of emerged and emerging technologies has a few basic foundation principles. These will be addressed in this segment. The basics for this segment can be found in more details in (BLAC94) and (TERP98).

3.2.2.1 Connection-oriented and Connectionless Communications

Communication systems that employ the concepts of circuits and virtual circuits are said to be connection-oriented. Such systems maintain information about the users, such as their addresses and their

ongoing QOS needs. Often, these types of systems use state tables that contain rules governing the manner in which the user interacts with the network. While these state tables clarify the procedures between the user and the communication network, they do add overhead to the communication process.

In contrast, communication systems that do not employ circuits and virtual circuits are said to be connectionless systems. They are also known as datagram networks and are widely used throughout the industry. The principal difference between connection-oriented and connectionless operation is that connectionless protocols do not establish a virtual circuit for the end user communication process. Instead, traffic is presented to the service provider in a somewhat *ad hoc* fashion. Handshaking arrangements, mutual confirmations are minimal and perhaps nonexistent. The network service points and the network switches maintain no ongoing knowledge about the traffic between the two end users. State tables as seen with connection-oriented solutions are not maintained. Therefore, datagram services provide no *a priori* knowledge of user traffic and they provide no ongoing current knowledge of the user traffic — but they introduce less overhead.

3.2.2.2 Physical and Virtual Circuits

End users operating terminals, computers, and client equipment communicate with each other through a communication channel called the physical circuit. These physical circuits are also known by other names, such as channels, links, lines, and trunks. Physical circuits can be configured wherein two users communicate directly with each other through one circuit, and no one uses this circuit except these two users. They can operate this circuit in half-duplex or full-duplex. This circuit is dedicated to the users. This concept is still widely used in simple networks without serious bandwidth limitations.

In more complex systems, such as networks, circuits are shared with more than one user-pair. Within a network, the physical circuits are terminated at intermediate points at machines that provide relay services on another circuit. These machines are known by such names as switches, routers, bridges, gateways, etc. They are responsible for relaying the traffic between the communicating users. Since many communication channels have the capacity to support more than one user session, the network device, such as the switch, router, or multiplexer is responsible for sending and receiving multiple user traffic to/from a circuit.

In an ideal arrangement, a user is not aware that the physical circuits are being shared by other users. Indeed, the circuit provider attempts to make this sharing operating transparent to all users. Moreover, in this ideal situation, the user thinks that the circuit directly connects only the two communicating parties. However, it is likely that the physical circuit is being shared by other users.

The term "virtual circuit" is used to describe a shared circuit wherein the sharing is not known to the circuit users. The term was derived from computer architectures in which an end user perceives that a computer has more memory than actually exists. This other, additional virtual memory is actually stored on an external storage device.

There are three types of virtual circuits:

- **Permanent virtual circuits (PVC)** — A virtual circuit may be provisioned to the user on a continuous basis. In this case, the user has the service of the network any time. A PVC is established by creating entries in tables in the network nodes' databases. These entries contain a unique identifier of the user payload which is known by various names, such as a logical channel number (LCN), virtual channel identifier (VCI), or virtual path identifier (VPI).
- Network features such as throughput, delay, security, and performance indicators are also provisioned before the user starts with operations. If different types of services are desired, and if different destination endpoints must be reached, then the user must submit a different PVC identifier with the appropriate user payload to the network. This PVC is provisioned to the different endpoint, and perhaps with different services.
- **Switched virtual circuits (SVC)** — A switched virtual circuit is not preprovisioned. When a user wishes to obtain network services to communicate with another user, it must submit a connection

request packet to the network. It must provide the address of the receiver, and it must also contain the virtual circuit number that is to be used during the session. SVCs entail some delay during the setup phase, but they are flexible in allowing the user to select dynamically the receiving party and the negotiation of networking parameters on a call-by-call basis.

- **Semi-permanent virtual circuits** (**SPVC**) — With this approach, a user is preprovisioned, as in a regular PVC. Like a PVC, the network node contains information about the communicating parties and the type of services desired. But these types of virtual circuits do not guarantee that the users will obtain their level of requested service. In case of congested networks, users could be denied the service.

In a more likely scenario, the continuation of a service is denied because the user has violated some rules of the communications. Examples are higher bandwidth demand and higher data rates than agreed with the supplier.

3.2.2.3 Switching Technologies

Voice, video, and data signals are relayed in a network from one user to another through switches. This section provides an overview on prevalent switching technologies.

Circuit switching provides a direct connection between two networking components. Thus, the communicating partners can utilize the facility as they see it — within bandwidth and tariff limitations. Many telephone networks use circuit switching systems. Circuit switching provides clear channels; error checking, session establishment, frame flow control, frame formatting, selection of codes, and protocols are the responsibility of the users. Today, the traffic between communicating parties is usually stored in fast queues in the switch and switched on to an appropriate output line with time division multiplexing (TDM) techniques. This technique is known as circuit emulation switching (CES). In summary:

- Direct connection end-to-end
- No intermediate storage unless CES used
- Few value-added functions
- Modern systems use TDM to emulate circuit switching

Message switching was the dominating switching technology during the last two decades. The technology is still widely used in certain applications, such as electronic mail, but it is not employed in a backbone network. The switch is usually a specialized computer. It is responsible for accepting traffic from attached terminals and computers. It examines the address in the header of the message and switches the traffic to the receiving station. Due to the low number of switching computers, this technology suffers under backup problems, performance bottlenecks, and lost messages due to congestion. In summary:

- Use of store-end-forward technology
- Disk serves as buffers
- Extensive value-added functions
- Star topology due to expense of switches

Packet switching relays small pieces of user information to the destination nodes. Packet switching has become the prevalent switching technology of data communications networks. It is used in such diverse systems as private branch exchanges (PBXs), LANs, and even with multiplexers. Each packet only occupies a transmission line for the duration of the transmission; the lines are usually fully shared with other applications. This is an ideal technology for bursty traffic. Modern packet switching systems are designed to carry continuous, high-volume traffic as well as asynchronous, low-volume traffic, and each user is given an adequate bandwidth to meet service level expectations.

The concept of packet and cell switching is similar; each attempts to process the traffic in memory as quickly as possible. But cell switching is using much smaller PDUs relative to packet switching. The PDU size is fixed with cell switching. The PDU size may vary with packet switching. In summary:

- Hold-and-forward technology
- RAM serves as buffers
- Extensive value-added-functions for packet, but not many for cells

Switching will remain one of the dominating technologies in the telecommunications industry.

3.2.2.4 Routing Technologies

There are two techniques to route traffic within and between networks: source routing and non-source routing. The majority of emerging technologies use non-source routing.

Source routing derives its name from the fact that the transmitting device — the source — dictates the route of the protocol data unit (PDU) through a network or networks. The source places the addresses of the "hops" in the PDU. The hops are actually routers representing the internetworking units. Such an approach means that the internetworking units need not perform address maintenance, but they simply use an address in the PDU to determine the destination of the PDU.

In contrast, non-source routing requires that the interconnecting devices make decisions about the route. They don't rely on the PDU to contain information about the route. Non-source routing is usually associated with bridges and is quite prevalent in LANs. Most of the emerging new technologies implement this approach with the use of a VCI. This label is used by the network nodes to determine where to route the traffic.

The manner in which a network stores its routing information varies. Typically, routing information is stored in a software table, called a directory. This table contains a list of destination nodes. These destination nodes are identifiers with some type of network address. Along with the network address (or some type of label, such as a virtual circuit identifier) there is an entry describing how the router is to relay the traffic. In most implementations, this entry simply lists the next node that is to receive the traffic in order to relay it to its destination.

Small networks typically provide a full routing table at each routing node. For large networks, full directories require too many entries, and are expensive to maintain. In addition, the exchange of routing table information can impact the available bandwidth for user payload. These networks are usually subdivided into areas, called domains. Directories of routing information are kept separately in domains.

Broadcast networks contain no routing directories. Their approach is to send the traffic to all destinations.

Network routing control is usually categorized as centralized or distributed. Centralized uses a network control center to determine the routing of the packets. The packet switches are limited in their functions. Central control is vulnerable; a backup is absolutely necessary, which increases the operating expenses. Distributed requires more intelligent switches, but they provide a more resilient solution. Each router makes its own routing decisions without regard to a centralized control center. Distributed routing is also more complex, but its advantages over the centralized approach have made it the preferred routing method in most communications networks.

3.2.2.5 Multiplexing Technologies

Most of the emerged and emerging technologies use some form of multiplexing. Multiplexers accept low-speed voice or data signals from terminals, telephones, PCs, and user applications and combine them into one higher-speed stream for transmission effiency. A receiving multiplexer demultiplexes and converts the combined stream into the original lower-speed signals. There are various multiplexing techniques:

Frequency Division Multiplexing (FDM) — This approach divides the transmission frequency range into channels. The channels are lower frequency bands; each is capable of carrying communication traffic, such as voice, data, or video. FDM is widely used in telephone systems, radio systems, and cable television applications. It is also used in microwave and satellite carrier systems. FDM decreases the total bandwidth available to each user, but even the narrower bandwidth is usually sufficient for the users' applications. Isolating the bands from each other costs some bandwidth, but the simultaneous use outweighs this disadvantage.

Time Division Multiplexing (TDM) — This approach provides the full bandwidth to the user or application, but divides the channel into time slots. Each user or application is given a slot and

the slots are rotated among the attached devices. The TDM multiplexer cyclically scans the input signals from the entry points. TDMs are working digitally. The slots are preassigned to users and applications. In case of no traffic at the entry points, the slots remain empty. This approach works well for constant bit rate applications, but leads to waste capacity for variable bit rate applications.

Statistical Time Division Multiplexing (STDM) — This approach allocates the time slots to each port on a STDM. Consequently, idle termninal time does not waste the capacity of the bandwidth. It is not unusual for two to five times as much traffic to be accomodated on lines using STDMs in comparison to a TDM solution. This approach can accomodate bursty traffic very well, but does not perform too well with continuous, nonbursty traffic.

Wave Division Multiplexing (WDM) — WDM is the optical equivalent of FDM. Lasers operating at different frequencies are used in the same fiber, thereby deriving multiple communications channels from one physical path. There is a more advanced form of this technology with even better efficiency, called Dense Wave Division Multiplexing (DWDM).

3.2.2.6 Addressing and Identification Schemes

In order for user traffic to be sent to the proper destination, it must be associated with an identifier of the destination. Usually, there are two techniques in use:

An explicit address has a location associated with it. It may not refer to a specific geographical location but rather a name of a network or a device attached to a network. For example, the Internet Protocol (IP) address has a structure that permits the identification of a network, a subnetwork attached to the network, and a host device attached to the subnetwork. The ITU-T X.121 address has a structure which identifies the country, a network within that country, and a device within the network. Other entries are used with these addresses to identify protocols and applications running on the networks. Explicit addresses are used by switches, routers, and bridges as an entry into routing tables. These routing tables contain information about how to route the traffic to the destination nodes.

Another identifying scheme is known by the term of label, although other terms may be more widely used. Those terms are logical channel number (LCN) or virtual circuit identifier (VCI). A label contains no information about network identifiers or physical locations. It is simply a value that is assigned which identifies each data unit of a user's traffic.

Almost all connectionless systems use explicit addresses, and the destination and source addresses must be provided with every PDU in order for it to be routed to the proper destination.

3.2.2.7 Control and Congestion Management

It is very important in communication networks to control the traffic at the ingress and egress points of the network. The operation by which user traffic is controlled by the network is called flow control. Flow control should assure that the traffic does not saturate the network or exceed the network's capacity. Thus, flow control is used to manage congestion.

There are three flow control alternatives with emerged and emerging technologies:

- Explicit flow control — This technique limits how much user traffic can enter the network. If the network issues an explicit flow control message to the user, the user has no choice but to stop sending traffic or to reduce traffic. Traffic can be sent again after the network has notified the user about the release of the limitations.
- Implicit flow control — This technique does not absolutely restict the flow. Rather, it recommends that the user reduce or stop traffic it is sending to the network if network capacity situations require a limitation. Typically, the implicit flow control message is a warning to the user that the user is violating its service level agreement with the internal or external supplier regarding network congestion. In any case, if the user continues to send traffic, it risks having traffic discarded by the network.
- No flow control — Flow control may also be established by not controlling the flow at all. Generally, an absence of flow control means that the network can discard any traffic that is creating problems. While this approach certainly provides superior congestion management from the standpoint of the network, it may not meet the performance expectations of the users.

3.2.3 Management Solutions for Emerged Technologies

The present status for emerged technologies, such as private leased lines, voice networks, SS7-based signalling techniques, message and packet switching, can be summarized as follows:

- Proprietary solutions dominate: this means that the management protocols selected are controlled by the supplier of the equipment or facilities vendors.
- Re-engineered by SNMP: many of the equipment vendors include SNMP agents into their devices to meet the requirements of customers. The SNMP agents provide information for performance management and reporting, but they usually do not change the real-time processing of status data within the devices.
- The management structures are very heterogeneous: in most cases, these structures are hierarchical including a manager of managers. This manager is using a proprietary architecture. Most of the interfaces to element managers and managed devices are proprietary.
- TMN has a very low penetration: suppliers have recognized the need for a generic standard, but they are not willing to invest heavily into supporting it. Some of the providers go as supporting the Q3-interface.
- Operating Support Systems are heavy: the legacy-type OSSs support the emerged technologies on behalf of the suppliers well, but they are flexible enough to address future needs. They lack in separating operations functionality from operations data, in using flexible software, and in separating network management from service management.

3.2.4 Emerging Technologies

This segment gives an overview on telecommunication technologies that are either in use but still considered new technology, or are considered for near-future implementation. These technologies include frame relay, FDDI, SMDS, ATM, Sonet/SDH, and mobile and wireless communications. The capabilities of these technologies are presented using the same format, including technology description flowed by evaluating management capabilities.

3.2.4.1 Frame Relay

The purpose of a frame relay network is to provide an end user with a high-speed virtual private network (VPN) capable of supporting applications with large bit-rate transmission requirements. It gives a user T1/E1 access rates at a lesser cost than can be obtained by leasing comparable T1/E1 lines. It is actually a virtually meshed network.

The design of frame relay networks is based on the fact that data transmission systems today are experiencing far fewer errors and problems than they did decades ago. During that period, protocols were developed and implemented to cope with error-prone transmission circuits. However, with the increased use of optical fibers, protocols that expend resources dealing with errors become less important. Frame relay takes advantage of this improved reliability by eliminating many of the now unnecessary error checking and correction, editing, and retransmission features that have been part of many data networks for almost two decades.

Frame relay has been working for many years. It represents a scaled-down version of LAPD. The flexibility of assigning bandwidth on demand is somewhat new. Frame relay is one of the alternatives of fast packet switching.

MIB availability

The frame relay objects are organized into three object groups:

- Data link connection management interface group
- Circuit group
- Error group

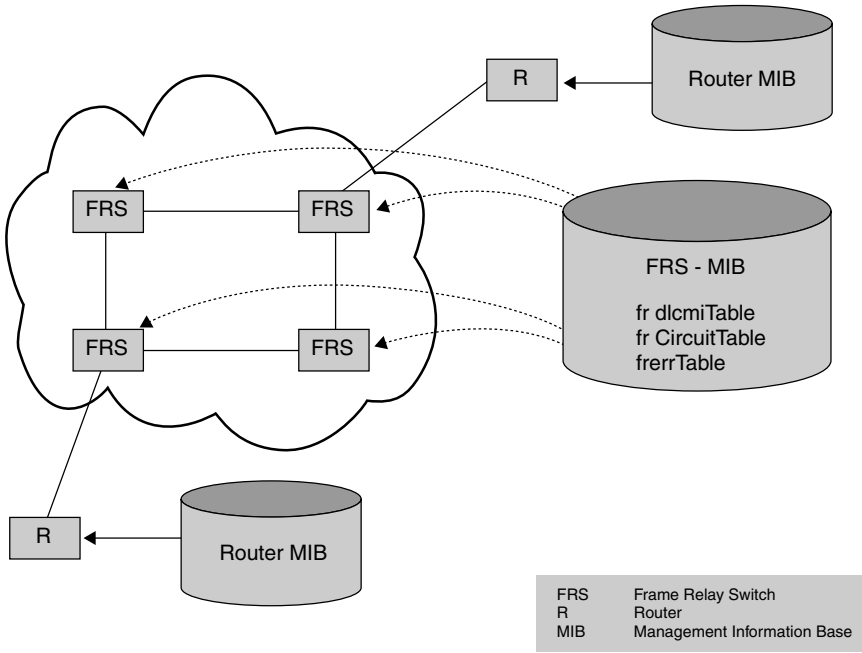

FIGURE 3.2.1 Communications paths between manager, agents, subagents, and managed objects.

These groups are stored in tables in the MIB and can be accessed by the SNMP manager. Figure 3.2.1 illustrates where SNMP operates, and lists the names of these three groups.

The frDlcmiTable contains 10 objects. Their purpose is to identify each physical port at the unified network interface (UNI), its IP address, the size of the DLCI header that is used on this interface, timers for invoking status and status inquiry messages, the maximum number of DLCIs supported at the interface, whether or not the interface uses multicasting, and miscellaneous operations.

The frCircuitTable contains 14 objects. Their purpose is to identify each PVC, its associated DLCI, if the DLCI is active, the number of BECNs and FECNs received since the PVC was created, statistics on the number of frames and octets sent and received since the DLCI was created, the DLCI's Bc and Be, and miscellaneous operations.

The third table is the frErrTable containing 4 objects. Their purpose is to store information on the types of errors that have occurred at the DLCI (unknown or illegal), and the time the error was detected. One object contains the header of the frame that created the error.

SNMP-based and proprietary solutions compete for management. Basically, each physical and logical component can be managed by periodically polling the PDUs in the MIB. Any powerful management platform can accomodate frame relay management, but the polling overhead over the wide area should be carefully controlled.

3.2.4.2 Fiber Distributed Data Interface (FDDI)

FDDI was developed to support high-capacity LANs. To obtain this goal, the original FDDI specifications stipulated the use of optical fiber as the transport media, although it is now available on twisted pair cable (CDDI). FDDI has been deployed in many corporations to serve as a high-speed backbone network for other LANs, such as Ethernet and Token Ring.

Basically, the standard operates with 100 Mbps rate. Dual rings are provided for the LAN, so the full speed is actually 200 Mbps, although the second ring is used typically as a backup to the primary ring. In practice. most installations have not been able to utilize the full bandwidth of FDDI. The standard defines multimode optical fiber, although single mode optical fiber can be used as well.

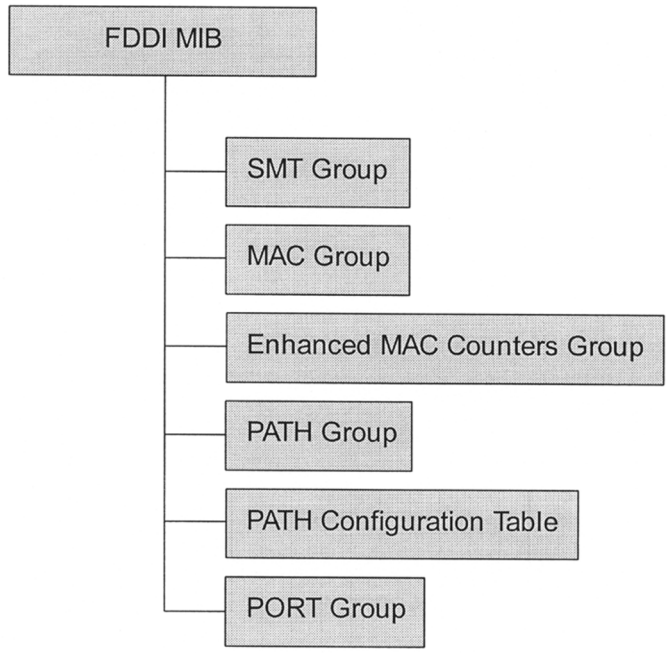

FIGURE 3.2.2 FDDI management information base.

FDDI was designed to make transmission faster on an optical fiber transport. Due to the high-capacity 100 Mbps technology, FDDI has a tenfold increase over the widely used Ethernet, and a substantial increase over Token Ring. FDDI was also to extend the distance of LAN interconnectivity. It permits the network topology to extend up to 200 km (14 miles).

FDDI II, which is able to incorporate voice, is not receiving enough industry interest.

FDDI is actually not a new technology, but internetworked FDDIs offer new alternatives in metropolitan areas competing with other technologies, such as frame relay and SMDS.

MIB Availability

The FDDI MIB has the following five groups (Figure 3.2.2):

- SMT Group — Contains a sequence of entries, one for each SMT implementation. The entries describe the station I.D., the operation I.D., the highest and lowest version I.D., the number of MACs in this station or concentrator, and other configuration and status information.
- MAC Group — A list of MAC tables, one for each MAC implementation across all SMTs. Each table describes the SMT index and the MIB-II If Index associated with this MAC, and status and configuration information for the given MAC.
- Enhanced MAC Counters Group — The MAC Counters table contains a sequence of MAC Counters entries. Each entry stores information about the number of tokens received, number of times TVX expired, number of received frames that have not been copied to the receive buffer, number of TRT expirations, number of times the ring entered operational status, and threshold information.
- PATH Group — Contains a sequence of PATH entries. Each entry starts with an index variable uniquely identifying the primary, secondary, and local PATH object instances. The entries also store information on different min and max time values for MACs in the given PATH.

- PATH Configuration Table — A table of path configuration entries. This table contains a configuration entry for all the resources that may be in this path.
- PORT Group — Contains a list of PORT entries. Each entry describes the SMT index associated with this port, a unique index for each port within the given SMT, the PORT type, and then neighbor type, connection policies, the list of permitted PATHs, the MAC number associated with the PORT (if any), the PMD entity class associated with this port and other capabilities and configuration information.

FDDI has its own management capabilities, defined in SMT, but they have never really taken off. Instead, suppliers are concentrating on SNMP capabilities. Using the MIB of FDDI agents, any SNMP manager can be used to manage FDDI.

3.2.4.3 Switched Multi-megabit Data Service

SMDS is a high-speed connectionless packet switching service which extends LAN-like performance beyond a subscriber's location. Its purpose is to ease the geographic limitations that exist with low-speed wide area networks. SMDS is designed to connect LANs, MANs, and also WANs.

The major goals of SMDS are to provide high-speed interfaces into customer systems, and at the same time allow customers to take advantage of their current equipment and hardware. Therefore, the SMDS operations are not performed by the end user machine; they are performed by customer promises equipment (CPE), such as a router.

SMDS is positioned as a service. If SMDS is considered unto itself, it is a new technology; it offers no new method for designing or building networks. This statement is emphasized because SMDS uses the technology of DQDB (dual queue dual bus), and then offers a variety of value-added services, such as bandwidth on demand, to the SMDS customer.

SMDS is targeted for large customers and sophisticated applications that need a lot of bandwidth, but not permanently. Generally, SMDS is targeted for data applications that transfer a lot of information in a bursty manner.

However, applications that use SMDS can be interactive. For example, two applications can exchange information interacting through SMDS, such as an X-ray, a document, etc. The restriction of SMDS is based on the fact that SMDS is not designed for real-time, full-motion video applications. Notwithstanding, it does support an interactive dialog between users, and allows them to exchange large amounts of information in a very short time. For example, it takes only one to two seconds for a high-quality color graphic image to be sent over a SMDS network. For many applications, this speed is certainly adequate.

MIB Availability

Figure 3.2.3 shows the location of the MIB in relation to the SMDS network. The SIP layers are also known in this figure to aid in reading the following material. The MIB is organized around managed objects which are contained in major groups. The groups, in turn, are defined in tables. As shown in the figure, at the bottom, the major entries in the MIB are the SMDS address, which is the conventional 60-bit address preceded by the 4 bits to signify individual group addresses. Thereafter, the groups are listed with their object identifier name. These names will be used in this segment to further describe the entries.

The sipL3Table contains the layer 3 (L3-PDU) parameters used to manage each SIP port. It contains entries such as port numbers, statistics on received traffic, information on errors such as unrecognized addresses, as well as various errors that have occurred at this interface.

The sipL2Table, as its name implies, contains information about layer 2 (L2-PDU) parameters and the state variables associated with information on the amount of the number of level 2 PDUs processed, error information such as violation of length of PDU, sequence number errors, MID errors, etc.

The sipDS1PLCP Table contains information on DS1 parameters and state variables for each port. The entries in the table contain error information such as DS1 severely erred framing seconds (SEFS), alarms, unavailable seconds encountered by the PLPC, etc.

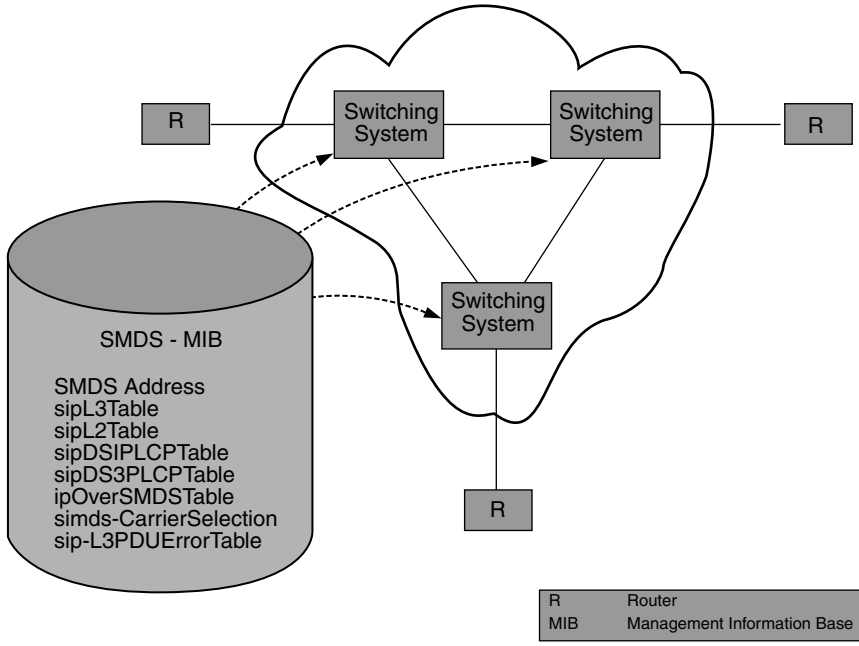

FIGURE 3.2.3 Structure of SNMP-based management services.

The sipDS3PLPC Table contains information about DS3 interfaces and state variables for each SIP port. Like its counterpart in DS1, this table contains information on severity-erred framing seconds, alarms, unavailable seconds, etc.

The ipOverSMDS Table contains information relating to operations of IP running on top of SMDS. It contains information such as the IP address, the SMDS address relevant to the IP station, addresses for ARP resolution, etc.

The smdsCarrierSelection group contains information on the inter-exchange carrier selection for the transport of traffic between LATAs.

Finally, the sipL3PDU Error Table contains information about errors encountered in processing the layer 3 PDU. Entries such as destination error, source error, invalid BAsize, invalid header extension, invalid PAD error, BEtag mismatch, etc. form the basis for this group.

As mentioned earlier, SNMP is used to monitor the MIBs and report on alarm conditions that have occurred based on the definitions in the MIBs.

SMDS management is expected to be ambitious. Switching systems are intelligent devices with the need of real-time decision making. In such situations, SNMP is not necessarily the right choice. However, SNMP may be used to transmit MIB entries to the manager for performance reporting.

3.2.4.4 Asynchronous Transfer Mode

The purpose of ATM is to provide a high-seed, low-delay, multiplexing and switching network to support any type of user traffic, such as voice, data, or video applications. ATM is one of four fast relay services. ATM segments and multiplexes user traffic into small, fixed-length units called cells. The cell is 53 octets, with 5 octets reserved for the cell header. Each cell is identified with virtual circuit identifiers that are contained in the cell header. An ATM network uses these identifiers to relay the traffic through high-speed switches from the sending CPE to the receiving CPE.

ATM provides limited error detection operations. It provides no retransmission services, and few operations are performed on the small header. The intention of this approach — small cells and with

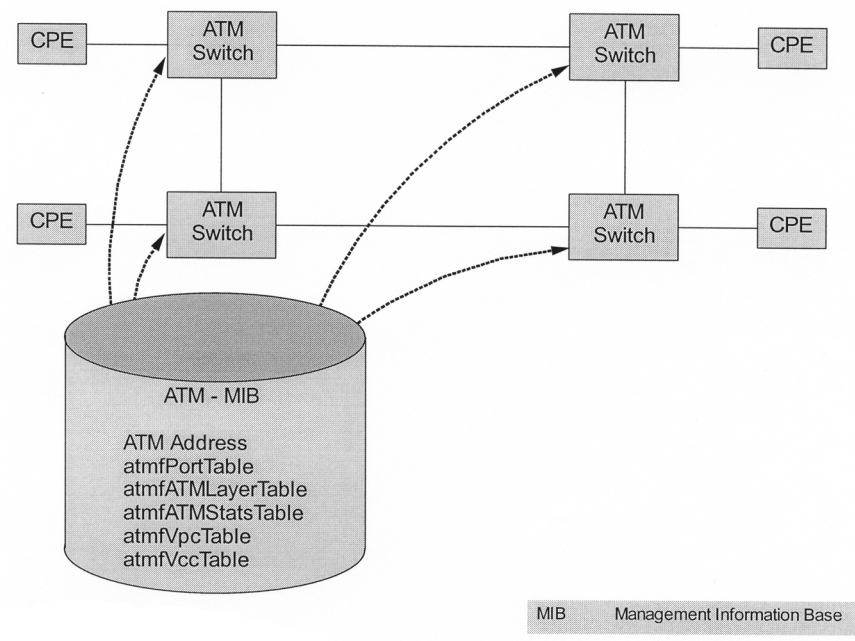

FIGURE 3.2.4 The ATM management information base.

minimal services performed — is to implement a network that is fast enough to support multimegabit transfer rates.

ATM is a new technology. ATM is supposed to be the foundation of providing the convergence, multiplexing, and switching operations. ATM resides on top of the physical layer.

MIB Availability

The ATM Forum has published a MIB as part of its Interim Local Management Interface Specification (ILMI) (Figure 3.2.4). The ATM MIB is registered under the enterprise node of the standard SMI in accordance with the Internet. MIB objects are therefore prefixed with 1.3.6.1.4.1.353.

Each physical link (port) at the UNI has a MIB entry that is defined in the atmfPortTable. This table contains a unique value for each port, an address, the type of port (DS3, SONET, etc.) media type (coaxial cable, fiber, etc.), status of port, (in service, out of service, etc.) and other miscellaneous objects.

The atmfAtmLayerTable contains information about the UNIs physical interface. The table contains: the port id, maximum number of VCCs, VPCs supported and configured on this UNI, active VCI/VPI bits on the UNI, and a description of public or private for the UNI.

The atmVpcTable and atmVccTable contain similar entries for the VPCs and VCCs, respectively, on the UNI. These tables contain the port id, VPI or VCI values for each connection, operational status (up, down, etc.), traffic shaping and policing descriptors (to describe the type of traffic management applicable to the traffic), and any applicable QoS that is applicable to the VPI or VCI.

The ATM Forum has defined two aspects of UNI network management:

- ATM layer management at the M plane, and
- Interim Local Management Interface (ILMI) specification.

M-Plane Management — Most of the functions for ATM M-plane management are performed with the SONET F1, F2, and F3 information flows. ATM is concerned with F3 and F4 information flows.

ILMI — Because the ITU-T and the ANSI have focused on C-plane and U-plane procedures, the ATM Forum has published a interim speficication called ILMI. The major aspects of ILMI are the use of SNMP

and a MIB. The ILMI stipulates the following procedures. First, each ATM device supports the ILMI, and one UNI ILMI MIB instance for each UNI. The ILMI communication protocol stack can be SNMP/UDP/IP/AAL over a well-known VPI/VCI value. SNMP is employed to monitor ATM traffic and the UNI VCC/VPC connections based on the ATM MIB with the SNMP get, Get-Next, Set, and Trap operations.

3.2.4.5 Sonet and SDH

Sonet/SDH is an optical-based carrier (transport) network utilizing synchronous operations between the network components. The term Sonet is used in North America, and SDH is used in Europa and Japan. Attributes of this technology are:

- A transport technology that provides high availability with self-healing topologies
- A multivendor that allows multivendor connections without conversions between the vendors' systems
- A network that uses synchronous operations with powerful multiplexing and demultiplexing capabilities
- A system that provides extensive OAM&P services to the network user and administrator

Sonet/SDH provides a number of attractive features when compared with current technology. First, it is an integrated network standard on which all types of traffic can be transported. Second, the Sonet/SDH standard is based on the optical fiber technology which provides superior performance in comparison to microwave and cable systems. Third, because Sonet/SDH is a worldwide standard, it is now possible for different vendors to interface their equipment without conversion.

Fourth, Sonet/SDH efficiently combines, consolidates, and segregates traffic from different locations through one facility. This concept, known as grooming, eliminates back hauling and other inefficient techniques currently being used in carrier networks. Back hauling is a technique in which user payload is carried past a switch that has a line to the user and sent to another endpoint. Then, the traffic to the other user is dropped, and the first users' payload is sent back to the switch and relayed back to the first user. In present configurations, grooming is eliminated, but expensive configurations, such as back-to-back multiplexers that are connected with cables, panels, or electronic cross-connect equipment are required.

Fifth, Sonet/SDH eliminates back-to-back multiplexing overhead by using new techniques in the grooming process. These techniques are implemented in a new type of equipment, called an add-drop multiplexer (ADM).

Sixth, the synchronous aspect of Sonet/SDH makes for more stable network operations. These types of networks experience fewer errors than the older asynchronous networks, and provide much better techniques for multiplexing and grooming payloads.

Seventh, Sonet/SDH has notably improved OAM&P features relative to current technology. Approximately 5% of the bandwidth is devoted to management and maintenance.

Eighth, Sonet/SDH employs digital transmission schemes. Thus, the traffic is relatively immune to noise and other impairments on the communications channel, and the system can use efficient TDM operations.

Sonet have been around a couple of years. The technology is not completely new, but its implementation is new.

MIB Availability

The Sonet/SDH MIB consists of eight groups. Each of the following groups have two tables: the Current Table and the Interval Table (Figure 3.2.5).

- The Sonet/SDH XXX Current Table contains various statistics that are being collected for the current 15-minute interval. The Sonet/SDH XXX Interval Table contains various statistics being collected by each system over a maximum of the previous 24 hours of operation. The past 24 hours may be broken into 96 completed 15-minute intervals. A system is required to store at least 4 completed 15-minute intervals. The default value is 32 intervals.

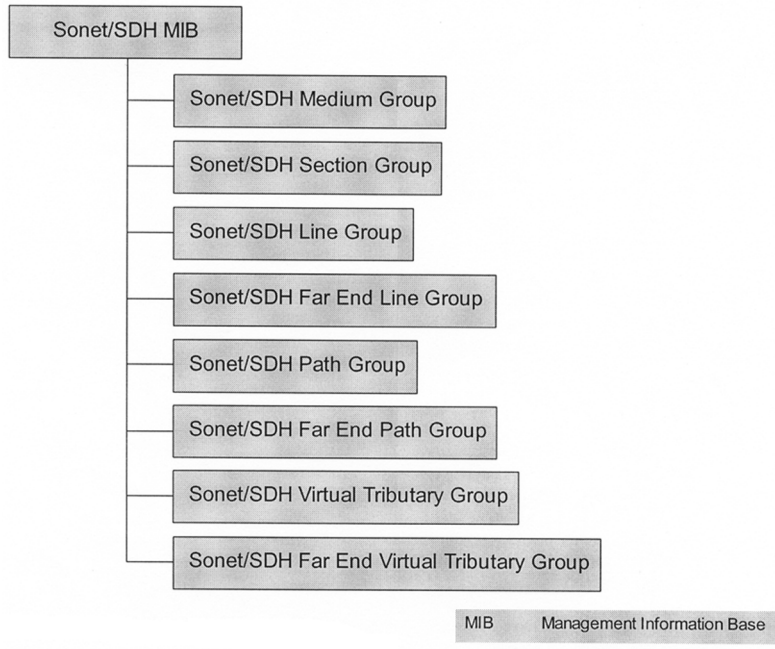

FIGURE 3.2.5 The Sonet/SDH management information base.

- The Sonet/SDH Medium Group: Sonet/SDH interfaces for some applications may be electrical interfaces and not optical interfaces. This group handles the configuration information for both optical Sonet/SDH interfaces and electrical Sonet/SDH interfaces, such as signal type, line coding, line type, and the like.
- The Sonet/SDH Section Group: This group consists of two tables:

  The Sonet/SDH Section Current Table and

  The Sonet/SDH Section Interval Table

  These tables contain information on interface status, counters on errored seconds, severely errored seconds, severely errored framing seconds, and coding violations.
- The Sonet/SDH Line Group: This group consists of two tables:

  The Sonet/SDH Line Current Table and

  The Sonet/SDH Line Interval Table

  These tables contain information on line status, counters on errored seconds, severely errored seconds, severely errored framing seconds, and unavailable seconds.
- The Sonet/SDH Far End Line Group: This group may only be implemented by Sonet/SDH (LTEs) systems that provide for far end block error (FEBE) information at the Sonet/SDH Line Layer. This group consists of two tables:

  The Sonet/SDH Far End Line Table and

  The Sonet/SDH Far End Line Interval Table
- The Sonet/SDH Path Group: This group consists of two tables:

  The Sonet/SDH Path Current Table and

  The Sonet/SDH Path Interval Table

  These tables contain information on interface status, counters on errored seconds, severely errored seconds, severely errored framing seconds, and coding violations.

- The Sonet/SDH Far End Path Group: This group consists of two tables:
  The Sonet/SDH Far End Path Current Table and
  The Sonet/SDH Far End Path Interval Table
- The Sonet/SDH Virtual Tributary Group: This group consists of two tables:
  The Sonet/SDH VT Current Table and
  The Sonet/SDH VT Interval Table

For SDH signals, virtual tributaries are called Vcs instead of Vts.

VT1.5	VC11
VT2	VC12
VT3	none
VT6	VC3

These tables contain information on virtual tributaries width and status, counters on errored seconds, severely errored seconds, severely errored framing seconds, and unavailable seconds.

- The Sonet/SDH Far End VT Group: This group consists of two tables:
  The Sonet/SDH Far End VT Current Table and
  The Sonet/SDH Far End VT Interval Table

The operation, administration, and maintenance (OAM) functions are associated with the hierarchical, layered design of Sonet/SDH. Figure 3.2.6 shows the five levels of the corresponding OAM operations, which are labeled F1, F2, F3, F4, and F5. F1, F2, and F3 functions reside at the physical layer; F4 and F5 functions reside at the ATM layer.

The Fn tags depict where the OAM information flows between two points, as shown in Figure 3.2.7.

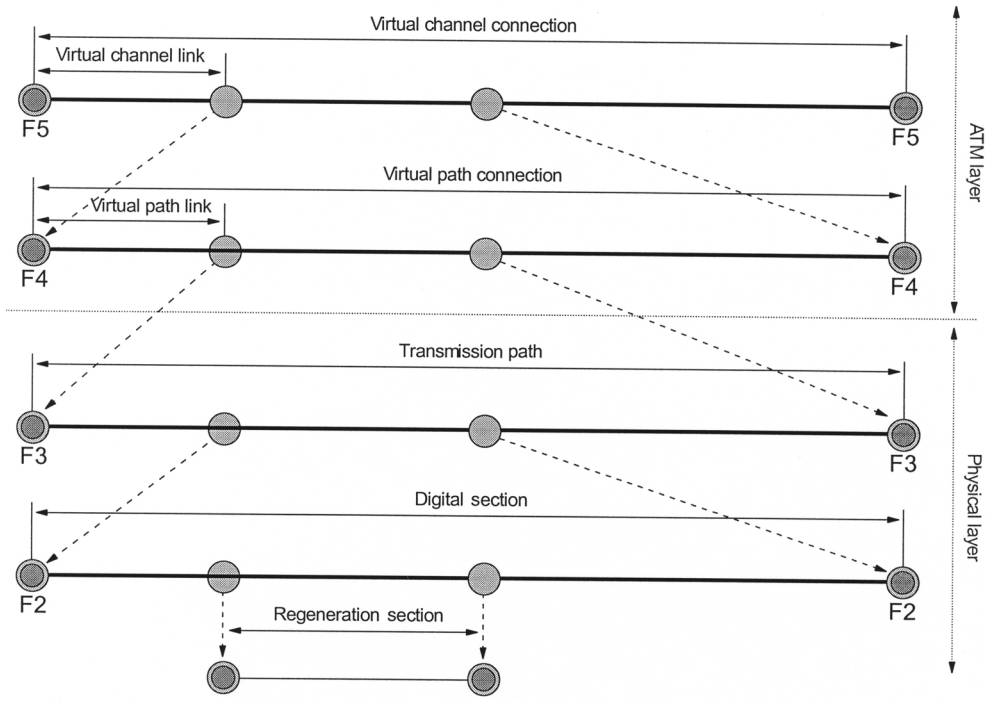

FIGURE 3.2.6 Relationships in ATM layers.