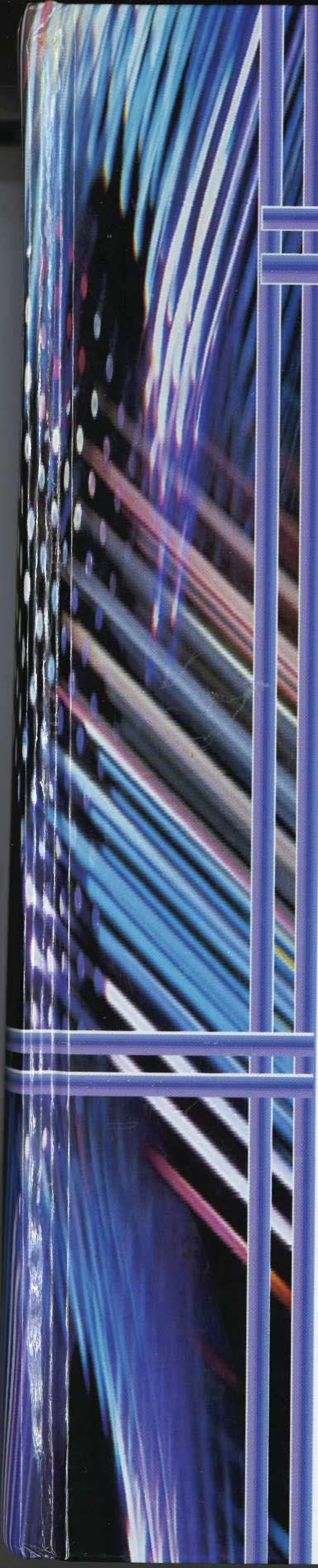
Includes latest SNMPv2 and RMON2 specs



SNMP SNMPv2 *and* RMON

Practical Network Management

Second Edition

William Stallings

ARRIS EX. 1024

Networking

SNMP, SNMPv2, *and* RMON

Practical Network Management

William Stallings

In order to manage today's complex, multivendor network environments effectively and to plan intelligently for the future, you will need an understanding of network management technology and a thorough grasp of the existing and evolving standards.

SNMP (Simple Network Management Protocol) is the most widely-deployed TCP/IP network management standard. This definitive guide is updated from the first edition to cover the final version of SNMPv2 and the increasingly popular RMON network management utility. It provides a comprehensive introduction to SNMP-based network management.

You will find clear explanations of such general network management fundamentals as performance monitoring and security control, as well as a specific introduction to SNMP network management concepts and information. Both the SNMPv1 and SNMPv2 protocols are described in depth. RMON2, the latest version of the Remote Network Monitoring management utility, is thoroughly documented, including practical techniques for its effective application.

Geared for network designers, implementors, and system managers, the book discusses critical design issues, explores various approaches to meeting communications requirements, and gives systems professionals the understanding they need to evaluate specific vendors' network products.

William Stallings heads his own consulting business, Comp-Comm Consulting, where he advises government agencies, computer and software vendors, and major users on the design, selection, and use of networking software and products. He is a frequent lecturer and author of numerous technical papers and books, including *Networking Standards: A Guide to OSI, ISDN, LAN, and MAN Standards* and *SNMP, SNMPv2, and CMIP: The Practical Guide to Network-Management Standards, First Edition.* He holds a PhD from MIT in Computer Science and a BS from Notre Dame in Electrical Engineering.

90000
9 780201 634792
ISBN 0-201-63479-1

Cover design by Avanda Peters
Cover art by Dominique Sarraute, The Image Bank
♻ Text printed on recycled paper
Corporate & Professional Group
Addison-Wesley Publishing Company

List of Acronyms

ACSE	Association Control Service Element
ANSI	American National Standards Institute
ASN.1	Abstract Syntax Notation One
FTP	File Transfer Protocol
IAB	Internet Architecture Board
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standardization
LAN	local-area network
MIB	management information base
OSI	Open Systems Interconnection
PDU	protocol data unit
RFC	Request for Comment
RMON	Remote Network Monitoring
SMI	structure of management information
SMP	Simple Management Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol

SNMP, SNMPv2, and RMON

SNMP, SNMPv2, and RMON
Practical Network Management

Second Edition

William Stallings

ADDISON-WESLEY PUBLISHING COMPANY
Reading, Massachusetts   Menlo Park, California   New York
Don Mills, Ontario   Wokingham, England   Amsterdam   Bonn
Sydney   Singapore   Tokyo   Madrid   San Juan
Seoul   Milan   Mexico City   Taipei

The publisher offers discounts on this book when ordered in quantity for special sales.

For more information, please contact:
Corporate & Professional Publishing Group
Addison-Wesley Publishing Company, Inc
One Jacob Way
Reading Massachusetts 01867

Library of Congress Cataloging-in-Publication Data

Stallings, William.
SNMP, SNMPv2, and RMON : practical network management / William Stallings. — 2nd ed.
p. cm.
Rev. ed. of: SNMP, SNMPv2, and CMIP, c1993.
Includes bibliographical references and index.
ISBN 0-201-63479-1
1. Computer networks—Management. 2. Computer network protocols—Standards. 3. Simple Network Management Protocol (Computer network protocol) I. Title.
TK5105.5.S732 1996
004.6'2—dc20 96-5916
CIP

0-201-63479-1
1 2 3 4 5 6 7 8 9-MA-99989296
First Printing July 1996

As always,
for ***Tricia Antigone***
and for **Geoffroi**, *too*

Contents

Part II SNMPv1

Part III RMON

Preface

The relentless growth in the information-processing needs of organizations has been accompanied both by the rapid development in computer- and data-networking technology to support those needs and by an explosion in the variety of equipment and networks offered by vendors. Gone are the days when an organization would rely on a single vendor and a relatively straightforward architecture to support its needs. The world is no longer divided into the pure mainframe-based, IBM-compatible, centralized environment and the PC-based, single-LAN-type, distributed environment. Today's typical organization has a large and growing but amorphous network architecture, with a variety of local-area networks (LANs) and wide-area networks (WANs), supported by bridges and routers, and a variety of distributed computing services and devices, including PCs, workstations, and servers. And, of course, despite over two decades of premature eulogies, the mainframe lives on in countless distributed and some centralized configurations.

To manage these systems and networks, which continue to grow in scale and diversity, a rich set of automated network management tools and applications is needed. Fundamental to the operation of such tools and applications in a multivendor environment are standardized techniques for representing and exchanging information relating to network management.

In response to these needs, managers and users have turned overwhelmingly to one standard: the Simple Network Management Protocol (SNMP) and the related Remote Network Monitoring (RMON) specification. SNMP was initially specified in the late 1980s and quickly became the standard means for multivendor network management. However, SNMP was too limited to meet all the critical needs for network management. Two enhancements have solidified the role of SNMP as the indispensable network management tool. First, the RMON specification, which is built on SNMP, was released in 1991. RMON defines algorithms and data bases for managing remote LANs. Second, an enhanced version of SNMP, known as SNMPv2, was released in 1993. SNMPv2 provides more functionality and greater efficiency than the original version of SNMP.

In 1996 both RMON and SNMPv2 were updated and extensively revised. This book is based on these most recent versions.

Objective

In order to manage today's systems effectively and to plan intelligently for the future use of network management systems, the systems manager needs an understanding of the technology of network management and a thorough grasp of the details of the existing and evolving standards. It is the objective of this book to fill this need.

This book provides a comprehensive introduction to SNMP-based network and internetwork management. The first part of the book is a survey of network management technology and techniques, to enable the reader to place the various vendor offerings into the context of his or her requirements. The second part of the book presents the original SNMP family of standards, which is still the most widely deployed version. The third part looks at the revised version of RMON, which includes an update of the original RMON specification, plus RMON2, which extends RMON functionality. The final part of the book examines SNMPv2 in detail. Throughout, practical issues related to the use of these standards and products based on these standards are examined.

Intended Audience

This book is intended for a broad range of readers interested in network management, including

- *Students and professionals in data processing and data communications:* This book is intended as a basic tutorial and reference source for this exciting area.
- *Network management designers and implementors:* This book discusses critical design issues and explores approaches to meeting communication requirements.
- *Network management system customers and system managers:* This book helps the reader understand what features and structures are needed in a network management facility and provides information about current and evolving standards to enable the reader to assess a specific vendor's offering.

Acknowledgments

I would like to thank the reviewers of this book, who generously provided feedback on part or all of the manuscript: K. K. Ramakrishnan of AT&T; Russell Dietz of Technically Elite Concepts; Ravi Prakash of FTP Software; Ole Jacobsen of Interop Company; Clif Baker of the Research Libraries Group; Sandra Durham of Cisco; and Ian Taylor of Cygnus. In addition, the two main authors of RMON2—Andy Bierman of Bierman Consulting, and Robin Iddon of AXON Networks—provided detailed reviews of the RMON material.

Also, I am grateful to the people who reviewed both the original proposal for this book and an early draft: Lyman Chapin of BBN; Radia Perlman of Novell; Glen Glater, Christopher Heigham, and Peter Schmidt of Midnight Networks.

How to Read This Book

Chapter 1 provides an overview of the concepts used throughout this book and includes a chapter-by-chapter summary. Following this introductory chapter, the book consists of four parts and two supporting appendices. The accompanying figure (Figure P.1: *A Reading Guide*) provides a suggested reading strategy for the book.

If you are unfamiliar with network management concepts, or have only a superficial understanding, you should read Part I (Chapters 2 and 3), which provides a basic introduction to the fundamentals of network management technology.

SNMP was developed for use in a TCP/IP environment, and the reader unfamiliar with this protocol suite should read Appendix A, which provides an overview. The SNMP and RMON specifications rely heavily on the use of Abstract Syntax Notation One (ASN.1), including the macro facility. The reader not up to speed on this notation should consult Appendix B before proceeding.

Part II (Chapters 4 through 7) deals with version 1 of SNMP and related MIBs. The remainder of the book builds on this part.

Parts III and IV can be read in either order. Part III (Chapters 8, 9, and 10) deals with remote monitoring (RMON), which is an important facility that can be provided with SNMP. RMON2, discussed in Chapter 10, makes use of some of the notation from SNMPv2 in its definitions. However, RMON2 can be used with an SNMPv1 infrastructure and does not require implementation of SNMPv2. The few references to SNMPv2 are explained in Chapter 10 so that Part III can be read independently of Part IV. Part IV (Chapters 11, 12, and 13) covers SNMP version 2 (SNMPv2).

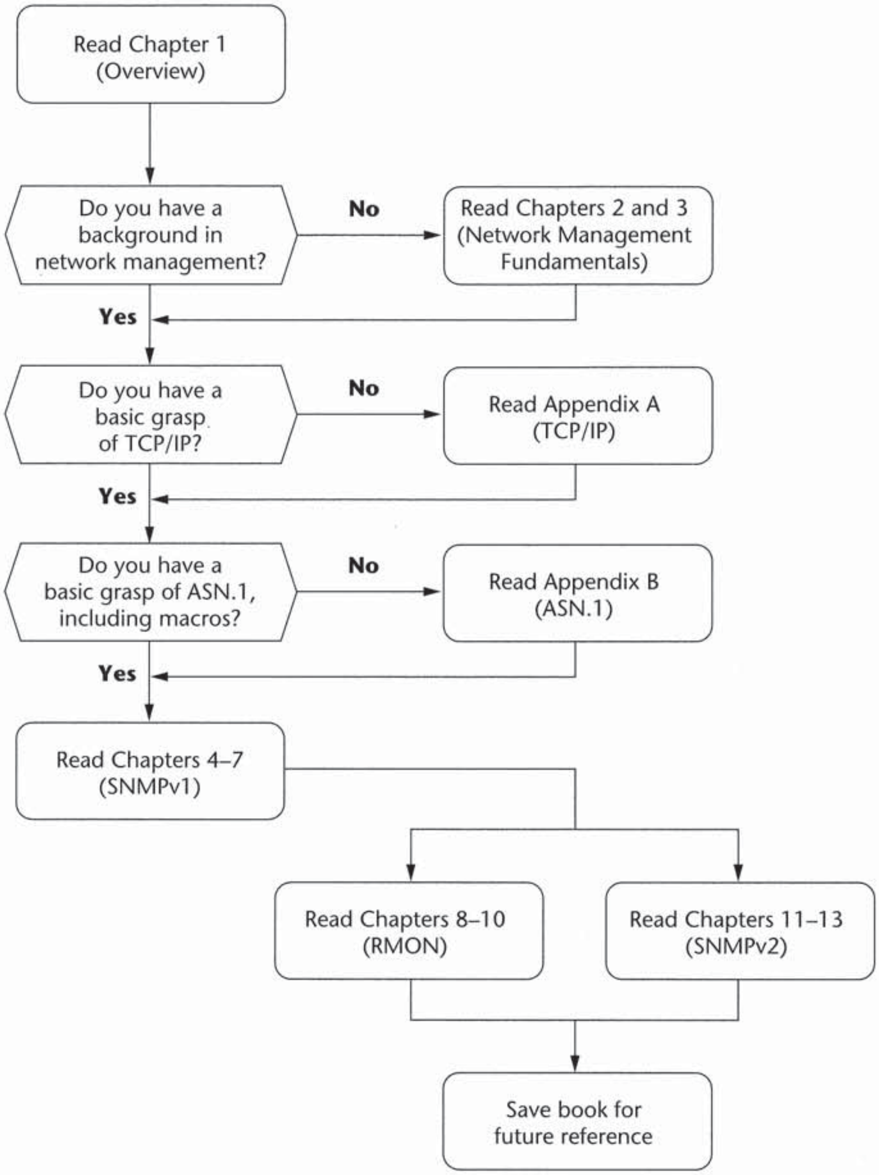

Read Chapter 1 (Overview)
Do you have a background in network management?
No
Read Chapters 2 and 3 (Network Management Fundamentals)
Yes
Do you have a basic grasp of TCP/IP?
No
Read Appendix A (TCP/IP)
Yes
Do you have a basic grasp of ASN.1, including macros?
No
Read Appendix B (ASN.1)
Yes
Read Chapters 4–7 (SNMPv1)
Read Chapters 8–10 (RMON)
Read Chapters 11–13 (SNMPv2)
Save book for future reference

FIGURE P.1 **A Reading Guide**

CHAPTER 1

Overview

Networks and distributed processing systems are of growing importance and, indeed, have become critical in the business world. Within a given organization, the trend is toward larger, more complex networks supporting more applications and more users. As these networks grow in scale, two facts become painfully evident:

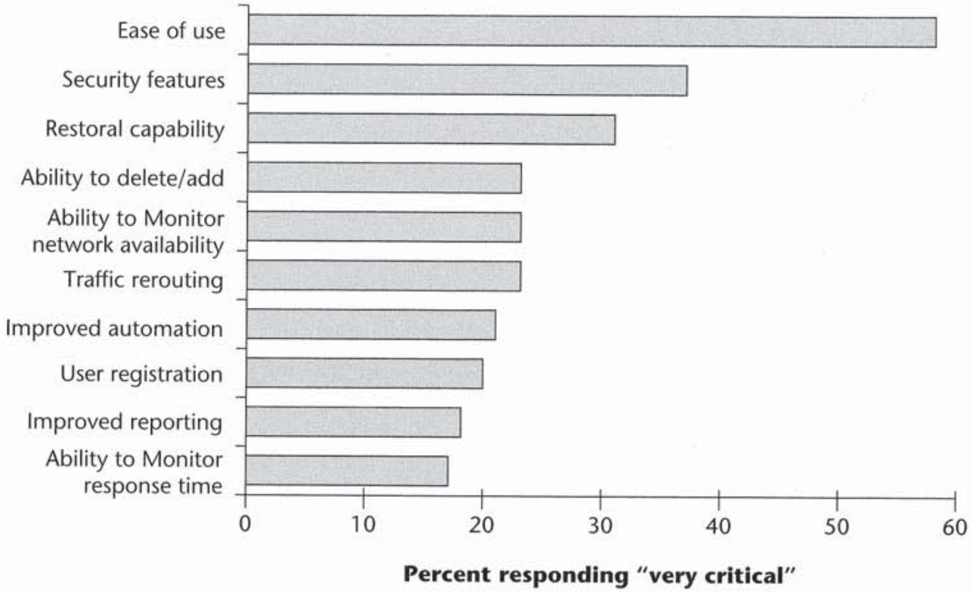
- The network and its associated resources and distributed applications become indispensable to the organization.
- More things can go wrong, disabling the network or a portion of the network, or degrading performance to an unacceptable level.

A large network cannot be put together and managed by human effort alone. The complexity of such a system dictates the use of automated network management tools. The urgency of the need for such tools—and the difficulty in supplying them—is increased if the network includes equipment from multiple vendors.

As networked installations become larger, more complex, and more heterogeneous, the cost of network management rises. To control costs, standardized tools are needed that can be used across a broad spectrum of product types, including end systems, bridges, routers, and telecommunications equipment, and that can be used in a mixed-vendor environment. In response to this need, the **Simple Network Management Protocol (SNMP)** was developed to provide a tool for multivendor, interoperable network management.

SNMP actually refers to a set of standards for network management, including a protocol, a database structure specification, and a set of data objects. SNMP was adopted as the standard for TCP/IP-based internets in 1989 and has enjoyed widespread popularity. In 1991 a supplement to SNMP, known as **Remote Network Monitoring (RMON)**, was issued; RMON extends the capabilities of SNMP to include management of local-area networks (LANs) as well as the devices attached to those networks. In 1993 an upgrade to SNMP, known as **SNMP version 2 (SNMPv2)**, was proposed; a revision of SNMPv2 was issued in 1996. SNMPv2 adds functional enhancements to SNMP and codifies the use of SNMP on OSI-based networks. Also in 1996, RMON was extended with an addition known as **RMON2.**

The bulk of this book is devoted to a study of SNMP, RMON, and SNMPv2, and to some of the practical issues associated with each. The remainder of this chapter, and the next two, provide an overview of network management in general.



[1]FIGURE 1.1 **Important Network Management Features**

1.1 *Network Management Requirements*

With any design, it is best to begin with a definition of the users' requirements. This is certainly true of an area as complex as network management. One way to do this is to consider the features that are most important to the user. Figure 1.1 shows the results of a recent survey. Given the cost of network management—and the magnitude of the task—it should be no surprise that ease of use is by far of most critical importance to users.[2]

Another breakdown of users' requirements is provided in (Terplan 1992), which lists the following as the principal driving forces for justifying an investment in network management:

- *Controlling corporate strategic assets:* Networks and distributed computing resources are increasingly vital resources for most organizations. Without effective control, these resources do not provide the payback that corporate management requires.
- *Controlling complexity:* The continued growth in the number of network components, end users, interfaces, protocols, and vendors threatens management with loss of control over what is connected to the network and how network resources are used.
- *Improving service:* End users expect the same or improved service as the information and computing resources of the organization grow and distribute.
- *Balancing various needs:* The information and computing resources of an organization must provide a spectrum of end users with various applications at given levels of support, with

TABLE 1.1 **OSI Management Functional Areas**

Fault management
The facilities that enable the detection, isolation, and correction of abnormal operation of the OSI environment

Accounting management
The facilities that enable charges to be established for the use of managed objects and costs to be identified for the use of those managed objects

Configuration and name management
The facilities that exercise control over, identify, collect data from, and provide data to managed objects for the purpose of assisting in providing for the continuous operation of interconnection services

Performance management
The facilities needed to evaluate the behavior of managed objects and the effectiveness of communication activities

Security management
The facilities that address those aspects of OSI security essential to operate OSI network management correctly and to protect managed objects

specific requirements in the areas of performance, availability, and security. The network manager must assign and control resources to balance these various needs.

- *Reducing downtime:* As the network resources of an organization become more important, minimum availability requirements approach 100 percent. In addition to proper redundant design, network management has an indispensable role to play in ensuring high availability of its resources.
- *Controlling costs:* Resource utilization must be monitored and controlled to enable essential end-user needs to be satisfied with reasonable cost.

While such surveys and qualitative statements are useful and can guide the designer in developing the details of a network management facility, a functional breakdown of requirements is needed to structure the overall design process. Table 1.1 lists the key functional areas of network management as defined by the International Organization for Standardization (ISO). Although this functional classification was developed for the OSI environment, it has gained broad acceptance by vendors of both standardized and proprietary network management systems.

1.1.1 Fault Management

1.1.1.1 Overview

To maintain the proper operation of a complex network, a network manager must take care that systems as a whole, and each essential component individually, are in proper working order. When a fault occurs, it is important, as rapidly as possible, for the network manager to

- Determine exactly where the fault is.
- Isolate the rest of the network from the failure so that it can continue to function without interference.
- Reconfigure or modify the network in such a way as to minimize the impact of operation without the failed component(s).
- Repair or replace the failed component(s) to restore the network to its initial state.

Central to the definition of fault management is the fundamental concept of a fault. Faults are to be distinguished from errors. A **fault** is an abnormal condition that requires management attention (or action) to repair, whereas an **error** is a single event. A fault is usually indicated by the failure to operate correctly or by excessive errors. For example, if a communications line is physically cut, no signals can get through. Or a crimp in the cable may cause wild distortions so that there is a persistently high bit-error rate. Certain errors (e.g., a single bit error on a communication line) may occur occasionally and are not normally considered to be faults. It is usually possible to compensate for errors using the error-control mechanisms of the various protocols.

1.1.1.2 User Requirements

End users expect fast and reliable problem resolution. Most end users will tolerate occasional outages. When these infrequent outages do occur, however, the end user generally expects to receive immediate notification and to have the problem corrected right away. To provide this level of fault resolution requires very rapid and reliable fault detection and diagnostic management functions. The impact and duration of faults can also be minimized by the use of redundant components and alternate communication routes, to give the network a degree of "fault tolerance." The fault management capability itself should be redundant to increase network reliability.

Users expect to be kept informed of the network status, including both scheduled and unscheduled disruptive maintenance. Users expect reassurance of correct network operation through mechanisms that use confidence tests or analyze dumps, logs, alerts, or statistics.

After correcting a fault and restoring a system to its full operational state, the fault management service must ensure that the problem is truly resolved and that no new problems are introduced. This requirement is called problem tracking and control.

As with other areas of network management, fault management should have a minimal effect on network performance.

1.1.2 Accounting Management

1.1.2.1 Overview

In many corporate networks, individual divisions or cost centers, or even individual project accounts, are charged for the use of network services. These are internal accounting procedures rather than actual cash transfers, but nevertheless they are important to the participating end users. Furthermore, even if no such internal charging is employed, the network manager needs to be able to track the use of network resources by end user or end-user class for a number of reasons, including the following:

- An end user or group of end users may be abusing its access privileges and burdening the network at the expense of other end users.
- End users may be making inefficient use of the network, and the network manager can assist in changing procedures to improve performance.
- The network manager is in a better position to plan for network growth if end-user activity is known in sufficient detail.

1.1.2.2 User Requirements

The network manager needs to be able to specify the kinds of accounting information to be recorded at various nodes, the desired interval between sending the recorded information to higher-level management nodes, and the algorithms to be used in calculating the charging. Accounting reports should be generated under network manager control.

In order to limit access to accounting information, the accounting facility must provide the capability to verify end users' authorization to access and manipulate that information.

1.1.3 Configuration and Name Management

1.1.3.1 Overview

Modern data communication networks are composed of individual components and logical subsystems (e.g., the device driver in an operating system) that can be configured to perform many different applications. The same device, for example, can be configured to act either as a router or as an end-system node, or both. Once it is decided how a device is to be used, the configuration manager can choose the appropriate software and set of attributes and values (e.g., a transport-layer retransmission timer) for that device.

Configuration management is concerned with initializing a network and gracefully shutting down part or all of the network. It is also concerned with maintaining, adding, and updating the relationships among components and the status of components themselves during network operation.

1.1.3.2 User Requirements

Startup and shutdown operations on a network are the specific responsibilities of configuration management. It is often desirable for these operations on certain components to be performed unattended (e.g., starting or shutting down a network interface unit).

The network manager needs the capability to identify the components that comprise the network and to define the desired connectivity of these components. Those who regularly configure a network with the same or a similar set of resource attributes need ways to define and modify default attributes and to load these predefined sets of attributes into the specified network components. The network manager must be able to change the connectivity of network components when end-users' needs change. The reconfiguration of a network is often desired in response to performance evaluation or in support of network upgrade, fault recovery, or security checks.

End users often need or want to be informed of the status of network resources and components. Therefore, end users should be notified when changes in configuration occur. Configuration reports can be generated either on some routine periodic basis or in response to a request for such a report. Before reconfiguration, end users often want to inquire about the upcoming status of resources and their attributes.

Network managers usually want only authorized end users (operators) to manage and control network operation (e.g., software distribution and updating).

1.1.4 Performance Management

1.1.4.1 Overview

Modern data communications networks are composed of many and varied components, which must intercommunicate and share data and resources. In some cases, it is critical to the effectiveness of an application that the communication over the network be within certain performance limits.

Performance management of a computer network comprises two broad functional categories—monitoring and controlling. **Monitoring** is the function that tracks activities on the network. The **controlling** function enables performance management to make adjustments to improve network performance. Some of the performance issues of concern to the network manager are as follows:

- What is the level of capacity utilization?
- Is there excessive traffic?
- Has throughput been reduced to unacceptable levels?
- Are there bottlenecks?
- Is response time increasing?

To deal with these concerns, the network manager must focus on some initial set of resources to be monitored in order to assess performance levels. This includes associating appropriate metrics and values with relevant network resources as indicators of different levels of performance. For example, what count of retransmissions on a transport connection is considered to be a performance problem requiring attention? Performance management, therefore, must monitor many resources to provide information in determining network operating level. By collecting this information, analyzing it, and then using the resultant analysis as feedback to the prescribed set of values, the network manager can become more and more adept at recognizing situations indicative of present or impending performance degradation.

1.1.4.2 User Requirements

Before using a network for a particular application, an end user may want to know such things as the average and worst-case response times and the reliability of network services. Thus performance must be known in sufficient detail to assess specific end-user queries. End users expect network services to be managed in a way that consistently affords their applications good response time.

Network managers need performance statistics to help them plan, manage, and maintain large networks. Performance statistics can be used to recognize potential bottlenecks before they cause problems so that appropriate corrective action can be taken. For example, the network manager can change routing tables to balance or redistribute traffic load during times of peak use or when a bottleneck is identified by a rapidly growing load in one area. Over the long term, capacity planning based on such performance information can indicate the proper decisions to make, for instance, with regard to an expansion of lines in that area.

1.1.5 Security Management

1.1.5.1 Overview

Security management is concerned with managing information protection and access-control facilities. These include generating, distributing, and storing encryption keys. Passwords and other authorization or access-control information must be maintained and distributed. Security management is also concerned with monitoring and controlling access to computer networks and to all or part of the network management information obtained from the network nodes. Logs are an important security tool, and security management is therefore very much involved with the collection, storage, and examination of audit records and security logs, as well as with the enabling and disabling of these logging facilities.

1.1.5.2 User Requirements

Security management provides facilities for the protection of network resources and end-user information. Network security facilities should be available for authorized users only. End users want to know that the proper security policies are in force and effective and that the management of security facilities is itself secure.

1.2 Network Management Systems

A **network management system** is a collection of tools for network monitoring and control that is integrated in the following ways:

- It contains a single operator interface with a powerful but user-friendly set of commands for performing most or all network management tasks.

- It has a minimal amount of separate equipment. That is, most of the hardware and software required for network management is incorporated into the existing user equipment.

A network management system consists of incremental hardware and software additions implemented among existing network components. The software used in accomplishing the network management tasks resides in the host computers and communications processors (e.g., front-end processors, terminal cluster controllers, bridges, and routers). A network management system is designed to view the entire network as a unified architecture, with addresses and labels assigned to each point and the specific attributes of each element and link known to the system. The active elements of the network provide regular feedback of status information to the network control center.

1.2.1 Network Management Configuration

Figure 1.2 suggests one possible architecture of a network management system. Each network node contains a collection of software devoted to the network management task, referred to in the diagram as a **network management entity (NME)**. Each NME performs the following tasks:

- collects statistics on communications and network-related activities
- stores statistics locally
- responds to commands from the network control center, including commands to
  1. transmit collected statistics to network control center
  2. change a parameter (e.g., a timer used in a transport protocol)
  3. provide status information (e.g., parameter values, active links)
  4. generate artificial traffic to perform a test

At least one host in the network is designated as the network control host, or **manager**. In addition to the NME software, the network control host includes a collection of software called the **network management application (NMA)**. The NMA includes an operator interface to allow an authorized user to manage the network. The NMA responds to user commands by displaying information and/or by issuing commands to NMEs throughout the network. This communication is carried out using an application-level network management protocol that employs the communications architecture in the same fashion as any other distributed application.

Other nodes in the network that are part of the network management system include an NME that responds to requests from a manager system. The NME in such managed systems is generally referred to as an agent module, or simply an **agent**. Agents are implemented in end systems that support end-user applications as well as nodes that provide a communications service, such as front-end processors, cluster controllers, bridges, and routers.

Several observations are in order:

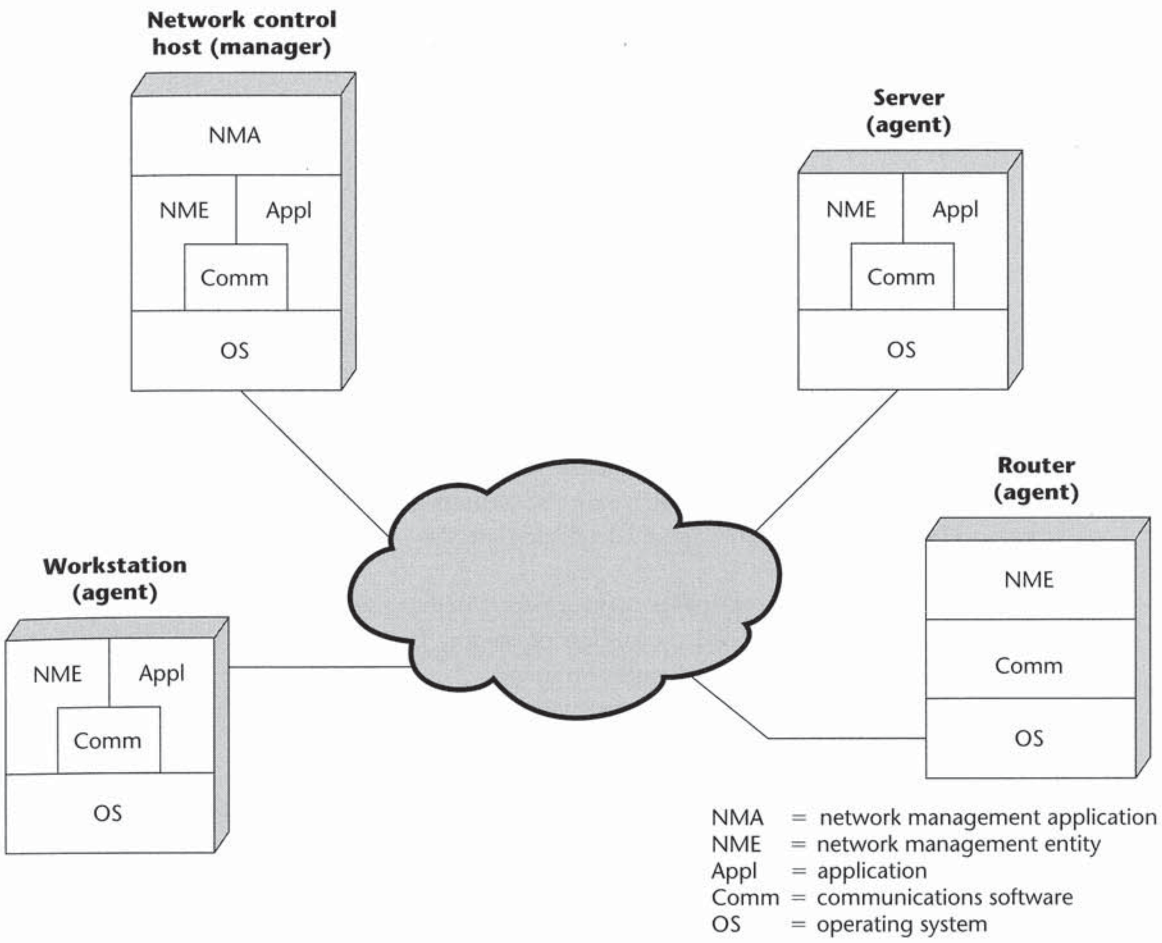


FIGURE 1.2 **Elements of a Network Management System**

1. Since the network management software relies on the host operating system and on the communications architecture, most offerings to date are designed for use on a single vendor's equipment. Recent years have seen the emergence of standardized network management systems designed to manage a multiple-vendor network.
2. As depicted in Figure 1.2, the network control host communicates with and controls the NMEs in other systems.
3. For maintaining high availability of the network management function, two or more network control hosts are used. In normal operation, one of the centers is idle or simply collecting statistics, while the other is used for control. If the primary network control host fails, the backup system can be used.

1.2.2 Network Management Software Architecture

The actual architecture of the network management software in a manager or agent varies greatly, depending on the functionality of the platform and the details of the network management capability. Figure 1.3 presents a generic view of such an architecture. The software can be divided into three broad categories:

- user presentation software
- network management software
- communications and database support software

1.2.2.1 User Presentation Software

Interaction between a user of network management and the network management software takes place across a user interface. Such an interface is needed in any manager system, to allow a user to monitor and control the network. It may also be useful to have such an interface in some agent systems for the purposes of testing and debugging and also to allow some parameters to be viewed or set locally.

The key to an effective network management system is a *unified* user interface. The interface should be the same at any node, regardless of vendor. This allows a user to manage a heterogeneous configuration with a minimum of training.

One danger in any network management system is information overload. It is possible to instrument a configuration so that a tremendous amount of information is available to the network management user. Presentation tools are needed to organize, summarize, and simplify this information as much as possible. Ideally, the emphasis will be on graphical presentations rather than textual or tabular outputs.

1.2.2.2 Network Management Software

The software that specifically provides the network management application may be very simple, as in the case of SNMP, or very complex, as in the case of OSI systems management. The central box in Figure 1.3 shows a rather complex structure that reflects the architecture of OSI systems management and also suggests a typical proprietary network management system.

The network management software in the figure is organized into three layers. The top layer consists of a collection of network management applications that provide the services of interest to users. For example, these applications could correspond to the OSI management functional areas: fault management, accounting management, configuration management, performance management, and security management. Each application covers a broad area of network management and should exhibit consistency over various types of configurations, although there may be detailed differences depending on the nature of the network facility (e.g., LAN, WAN, T1 multiplexer network).

The small number of network management applications is supported by a larger number of application elements. These are modules that implement more primitive and more general-

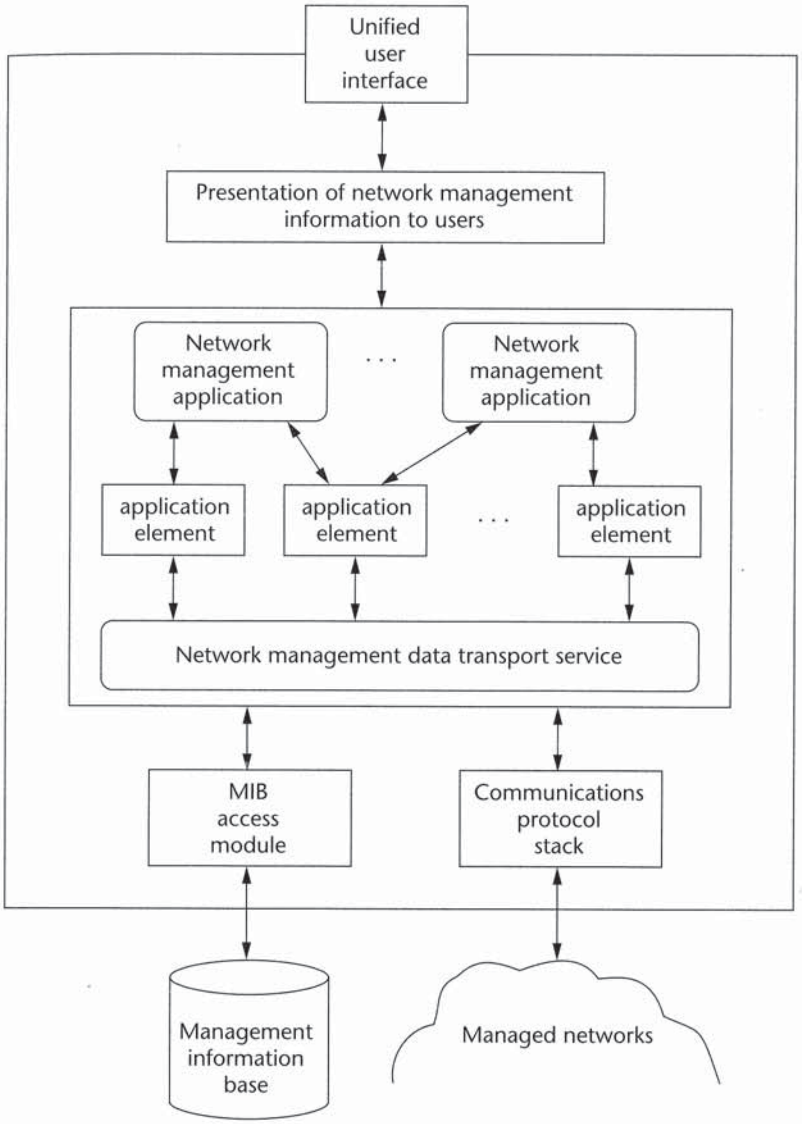

Unified user interface
Presentation of network management information to users
Network management application
. . .
Network management application
application element
application element
. . .
application element
Network management data transport service
MIB access module
Communications protocol stack
Management information base
Managed networks

FIGURE 1.3 **Architectural Model of a Network Management System**

purpose network management functions, such as generating alarms or summarizing data. The application elements implement basic tools that are of use to one or more of the network management applications. Organizing the software in terms of applications and application elements follows traditional modular design principles and enables a more efficient implementation to be developed based on software reuse.

The lowest level of management-specific software is a network management data transport service. This module consists of a network management protocol used to exchange management information among managers and agents and a service interface to the application elements. Typically, the service interface provides very primitive functions, such as get information, set parameters, and generate notifications.

1.2.2.3 Network Management Support Software

To perform its intended functions, network management software needs access to a local **management information base (MIB)** and to remote agents and managers. The local MIB at an agent contains information of use to network management, including information that reflects the configuration and behavior of this node, and parameters that can be used to control the operation of this node. The local MIB at a manager contains such node-specific information as well as summary information about agents under the manager's control. The MIB access module includes basic file management software that enables access to the MIB. In addition, the access module may need to convert from the local MIB format to a form that is standardized across the network management system.

Communications with other nodes (agents and managers) are supported by a communications protocol stack, such as OSI or the TCP/IP stack. The communications architecture thus supports the network management protocol, which is at an application level.

1.2.3 Distributed Network Management

The configuration depicted in Figure 1.2 suggests a centralized network management strategy, with a single network control center and perhaps a standby center. This is the strategy that both mainframe vendors and information system executives have traditionally favored. A centralized network management system implies central control. This makes sense in a mainframe-dominated configuration, where the key resources reside in a computer center and service is provided to remote users. The strategy also makes sense to managers responsible for the total information system assets of an organization. A centralized network management system enables the manager to maintain control over the entire configuration, balancing resources against needs and optimizing the overall utilization of resources.

However, just as the centralized computing model has given way to a distributed computing architecture, with applications shifted from data centers to remote departments, network management is also becoming distributed. The same factors come into play: the proliferation of low-cost, high-power PCs and workstations; the widespread use of departmental LANs; and the need for local control and optimization of distributed applications.

A distributed management system replaces the single-network control center with interoperable workstations located on LANs distributed throughout the enterprise. This strategy gives departmental-level managers, who must watch over downsized applications and PC LANs, the tools they need to maintain responsive networks, systems, and applications for their local end users. To prevent anarchy, a *hierarchical* architecture is typically used, with the following elements:

- Distributed management stations are given limited access for network monitoring and control, usually defined by the departmental resources they serve.
- One central workstation, with a backup, has global access rights and the ability to manage all network resources. It can also interact with less-enabled management stations to monitor and control their operations.

While maintaining the capacity for central control, the distributed approach offers a number of benefits:

1. Network management traffic overhead is minimized. Much of the traffic is confined to the local environment.
2. Distributed management offers greater scalability. Adding additional management capability is simply a matter of deploying another inexpensive workstation at the desired location.
3. The use of multiple networked stations eliminates the single point of failure that exists with centralized schemes.

Figure 1.4 illustrates the basic structure used for most distributed network management systems now on the market. The management clients are found closest to the users. These clients give the user access to management services and information and provide an easy-to-use graphical user interface. Depending on access privileges, a client workstation may access one or more management servers. The management servers are the heart of the system. Each server supports a set of management applications and a management information base (MIB). They also store common management-data models and route management information to applications and clients. Those devices to be managed that share the same network management protocol as the management servers contain agent software and are managed directly by one or more management servers. For other devices, management servers can reach the resources only through a vendor-specific element manager, or *proxy*. The concept of a proxy is explored in the next subsection.

The flexibility and scalability of the distributed management model are evident from Figure 1.4. As additional resources are added to the configuration, each is equipped with agent software or linked to a proxy. In a centralized system, this growth might eventually overwhelm a central station. But in a distributed system, additional management servers and client workstations can be added to cope with the extra resources. Furthermore, the growth of the overall configuration will occur in a structured way (e.g., adding an additional LAN with a number of attached PCs); the growth of the management system mirrors this underlying resource growth, with servers and clients added where the new resources are located.

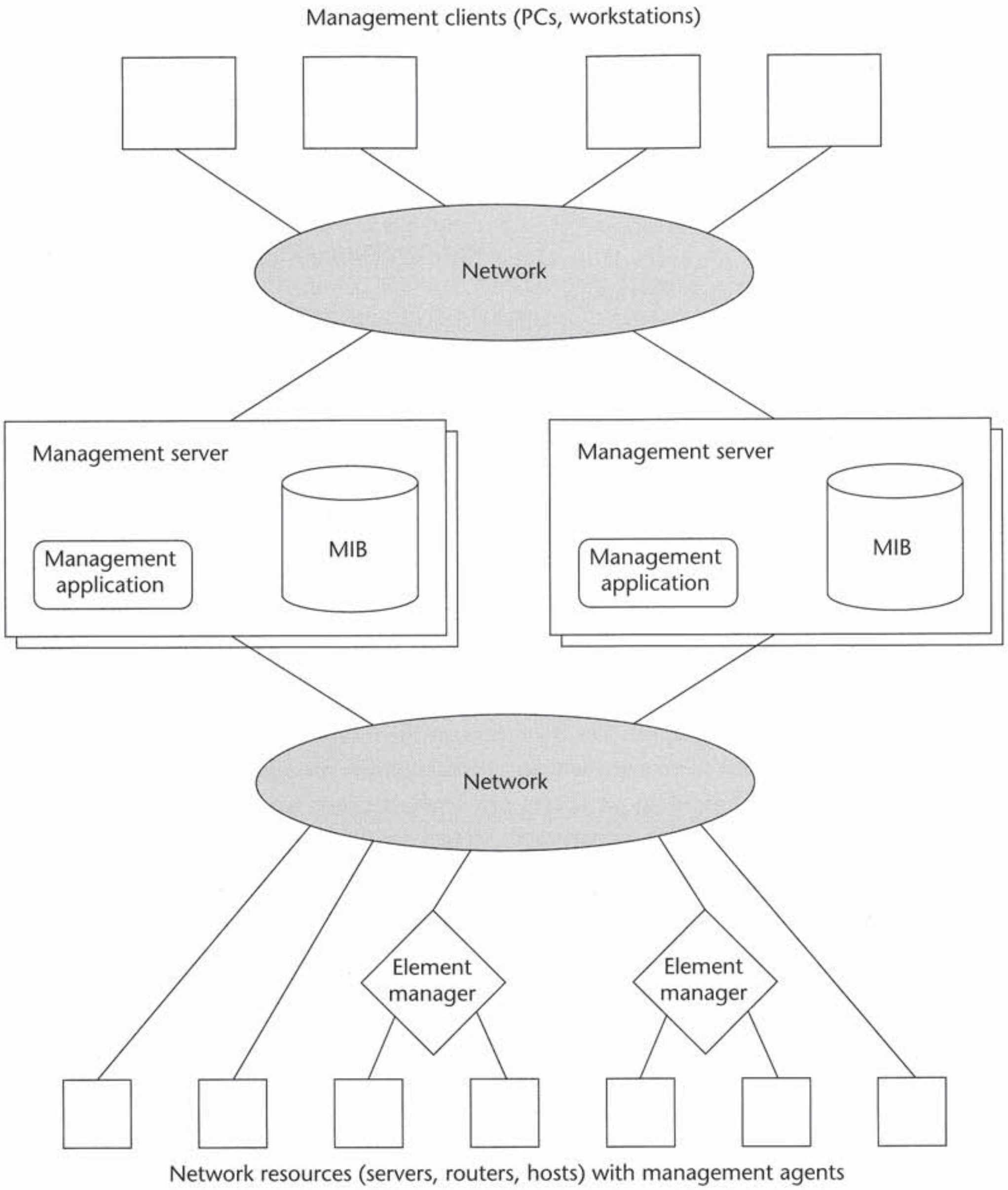


FIGURE 1.4 **Typical Distributed Management System Architecture**

1.2.4 Proxies

The configuration of Figure 1.2 suggests that each component that is of management interest includes a network management entity, with common network management software across all managers and agents. In an actual configuration, this may not be practical or even possible. For example, the configuration may include older systems that do not support the current network management standards, small systems that would be unduly burdened by a full-blown NME implementation, or components such as modems and multiplexers that do not support additional software.

To handle such cases, it is common to have one of the agents in the configuration serve as a **proxy** for one or more other nodes. We will have more to say about proxies in Part II, but for now we provide a brief introduction to the concept. When an agent performs in a proxy role, it acts on behalf of one or more other nodes. A network manager that wishes to obtain information from or control the node communicates with the proxy agent. The proxy agent then translates the manager's request into a form appropriate for the target system and uses an appropriate network management protocol to communicate with the target system. Responses from the target system back to the proxy are similarly translated and passed on to the manager.

Figure 1.5 illustrates a structured architecture that enables a management application to manage a proprietary resource through standard operations and event reports that are translated by the proxy system into proprietary operations and event reports. In this case, a **remote procedure call (RPC)** mechanism is used. The RPC mechanism is frequently found with distributed systems software and provides a flexible and easy-to-use facility for supporting the proxy function.

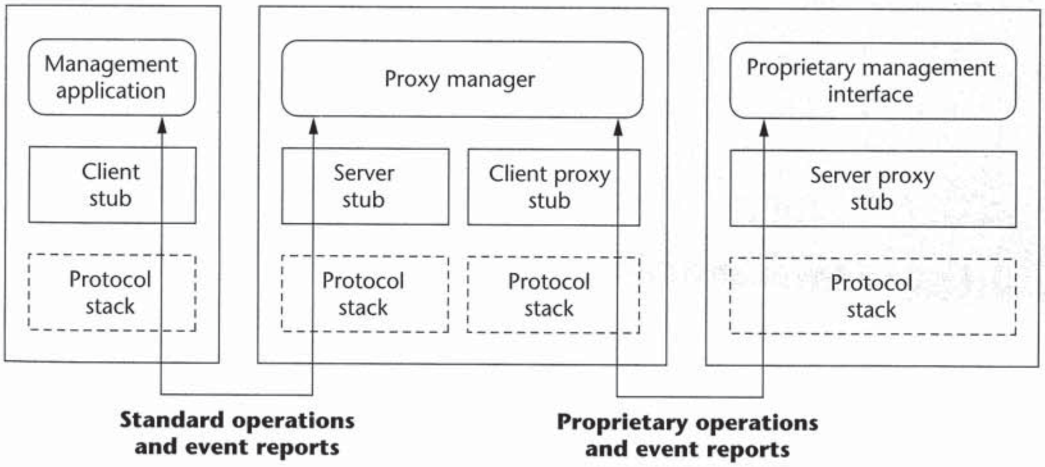


FIGURE 1.5 Proxy Manager Architecture

1.3 *Outline of the Book*

This chapter serves as an introduction to the entire book. A brief synopsis of the remaining chapters follows.

1.3.1 Chapter 2 Network Monitoring

Fundamental to network management is the ability to gather information about the status and behavior of the networked configuration, which is the function of network monitoring. Indeed, many network management systems provide only a network-monitoring capability. This chapter examines the basic architectural and design issues of network monitoring and then looks at three specific areas: performance monitoring, fault monitoring, and accounting monitoring.

1.3.2 Chapter 3 Network Control

A complete network management system will include the capability of controlling a configuration as well as monitoring it. Chapter 3 examines the basic mechanisms of network control and then looks at two aspects of network control: configuration control and security control.

1.3.3 Chapter 4 SNMP Network Management Concepts

A network management framework for TCP/IP-based internets has been developed and standardized for use in conjunction with the TCP/IP protocol suite. The framework includes the Simple Network Management Protocol (SNMP), a structure of management information, and a management information base. This chapter provides an overview of the concepts that underlie SNMP and the related standards.

1.3.4 Chapter 5 SNMP Management Information

Management information accessible via SNMP is maintained in a management information base (MIB) at each manager and agent node. This chapter summarizes the structure of SNMP management information, which consists of a simple, hierarchical structure of objects. Each object represents some attribute of a managed resource. The chapter looks at the formal methods for defining and representing management information and examines some of the practical issues in the use of such information in a multivendor, interoperable environment.

1.3.5 Chapter 6 Standard MIBs

Chapter 6 examines MIB-II, which is a structured set of standard objects that includes many of the objects commonly required in an SNMP-based network management system. It also describes the important Ethernet interface MIB, which along with MIB-II, is an Internet standard.

1.3.6 Chapter 7 Simple Network Management Protocol (SNMP)

This chapter reviews the basic principles of operation of SNMP. Then the protocol specification itself is examined in detail. The chapter also discusses the type of transport-level service that may be used to support SNMP and looks at the MIB objects used to monitor and manage the operation of the protocol itself.

1.3.7 Chapter 8 Remote Monitoring: Statistics Collection

A network management system is concerned not only with the status and behavior of individual nodes on a network, but also with the traffic on the network itself. "Remote monitoring" refers to the monitoring of a network by one of the nodes on the network, for the purposes of network management. In the context of SNMP, a remote monitoring (RMON) MIB has been defined. The RMON MIB specifies the information that is to be collected and stored by a remote monitor. The specification also defines the functionality of the monitor and the functionality of the manager—fjmonitor interaction. Chapter 8 introduces the fundamental concepts of RMON and then examines those elements of the RMON MIB that are principally concerned with statistics collection.

1.3.8 Chapter 9 Remote Network Monitoring: Alarms and Filters

Chapter 9 completes the discussion of the original RMON with a look at those elements associated with generating alarms on the basis of specified events and with filtering and capturing packet traffic. The chapter also looks at some of the practical issues involved in the use of RMON in a multivendor, interoperable environment.

1.3.9 Chapter 10 RMON2

This chapter examines the recent extension of the RMON MIB to encompass a broader range of managed objects. This extension of RMON, known as RMON2, focuses on traffic and addressing at protocol layers above the medium access-control (MAC) layer, with emphasis on IP traffic and application-level traffic.

1.3.10 Chapter 11 SNMPv2: Management Information

As its name suggests, SNMP provides a simple facility for network management, one that is easy to implement and should consume minimal processing resources. Many users of SNMP have felt the need for a more powerful and comprehensive facility, without going to the full-blown capability represented by OSI systems management. In response to this need, version 2 of SNMP (SNMPv2) was developed. SNMPv2 provides functional enhancements to SNMP as well as features that improve the efficiency of SNMP operation. This chapter examines the management information aspects of SNMPv2.

1.3.11 Chapter 12 SNMPv2: Protocol

This chapter provides a description of the SNMPv2 protocol, followed by a discussion of transport mappings defined for SNMPv2. Finally, the chapter examines strategies for the coexistence of SNMPv2 and SNMPv1 entities on the same network.

1.3.12 Chapter 13 SNMPv2: MIBs and Conformance

We begin this chapter with a description of the SNMPv2 MIB, which instruments both SNMPv2 and SNMPv1. Next conformance statements are examined; these are used to specify conformance requirements for standardized MIBs and to enable vendors to document the scope of their implementation. Finally, the chapter discusses the MIB extensions to the interfaces group, which are defined using SNMPv2 SMI and depend on some of the protocol features of SNMPv2.

1.3.13 Appendix A The TCP/IP Protocol Suite

This appendix summarizes the TCP/IP protocol suite, including the protocol architecture and each layer of the architecture.

1.3.14 Appendix B Abstract Syntax Notation One (ASN.1)

ASN.1 is the language used to define the syntax of objects in the management information base for both the SNMP family and OSI systems management. In addition, the syntax of application-level protocol data units for both the SNMP family and OSI systems management is defined using ASN.1. The basic elements of ASN.1 and examples of its use are provided in this appendix.

APPENDIX 1A INTERNET RESOURCES

It is the author's hope that this book will serve both as a tutorial for learning about the field of network management and as a reference for help on a specific topic. However, with the rapid changes taking place in both the technology and the standards for this field, no book can hope to stand alone for very long. The reader who is truly interested in this field will need to invest a certain amount of time keeping up with new developments. One of the best ways is through the Internet.

1A.1 Electronic Mailing Lists

A useful way to track developments in a particular area—and a forum for getting answers to questions—is to join an **electronic mailing list**. A mailing list is really nothing more than an alias that has multiple destinations. Mailing lists are usually created to discuss specific topics. Anyone interested in that topic may join that list.

A number of mailing lists are available on the Internet. Anyone directly connected to the Internet can participate in the Internet mailing lists. There are several common ways of joining a mailing list, as described below. Once you have been added to a list, you will receive a copy of every message posted to the list. If you wish to ask a question or respond to someone else's question, send a message to the list address. Your message will be posted to the list. As a member of the list, you will receive a copy of the message, which serves as a check that the message was posted.

Mailing lists should not be abused, since excessive messages clog the Internet and the mailbox of every member of the list. On the other hand, don't hesitate to ask even elementary questions that you can't answer yourself with the aid of available documentation. Generally, someone will take the time to answer.

For the purposes of this discussion, the following are noteworthy mailing lists:

- *SNMP mailing list:* This list serves as a discussion of topics related to SNMP. Currently, this is a very active list, covering details of existing SNMP implementations as well as questions about the SNMP standards. To subscribe, send an email message with the subject "subscribe" and a body containing your preferred email address to snmp-request@psi.com. Mailing address for messages: snmp@psi.com.
- *RMON mailing list:* This mailing list is devoted to the RMON (remote monitoring) portion of SNMP. To subscribe, send a message to "Majordomo@cisco.COM" with a body of "subscribe rmonmib". Mailing address for messages: rmonmib@cs.hmc.edu.

Important note: Do *NOT* send a subscription request to the mailing list itself (i.e., a subscribe message to snmp@psi.com). Such an action (1) will not get you on the list and (2) annoys the current subscribers who are forced to look at a futile attempt on your part to join them. By the same token, don't attempt to unsubscribe by sending the request to the mailing list.

1A.2 USENET News Groups

Another handy way to track developments and get questions answered is **USENET**, which is a collection of electronic bulletin boards that work in much the same way as the Internet mailing lists. If you subscribe to a particular news group, you will receive all messages posted to that group, and you may post a message that will be available to all subscribers. The differences between USENET and Internet mailing lists have to do with the mechanics of the systems. USENET is actually a distributed network of sites that collect and broadcast news group entries. To access a news group, for read or write, one must have access to a USENET node. Such nodes are accessible over the Internet, and in a variety of other ways.

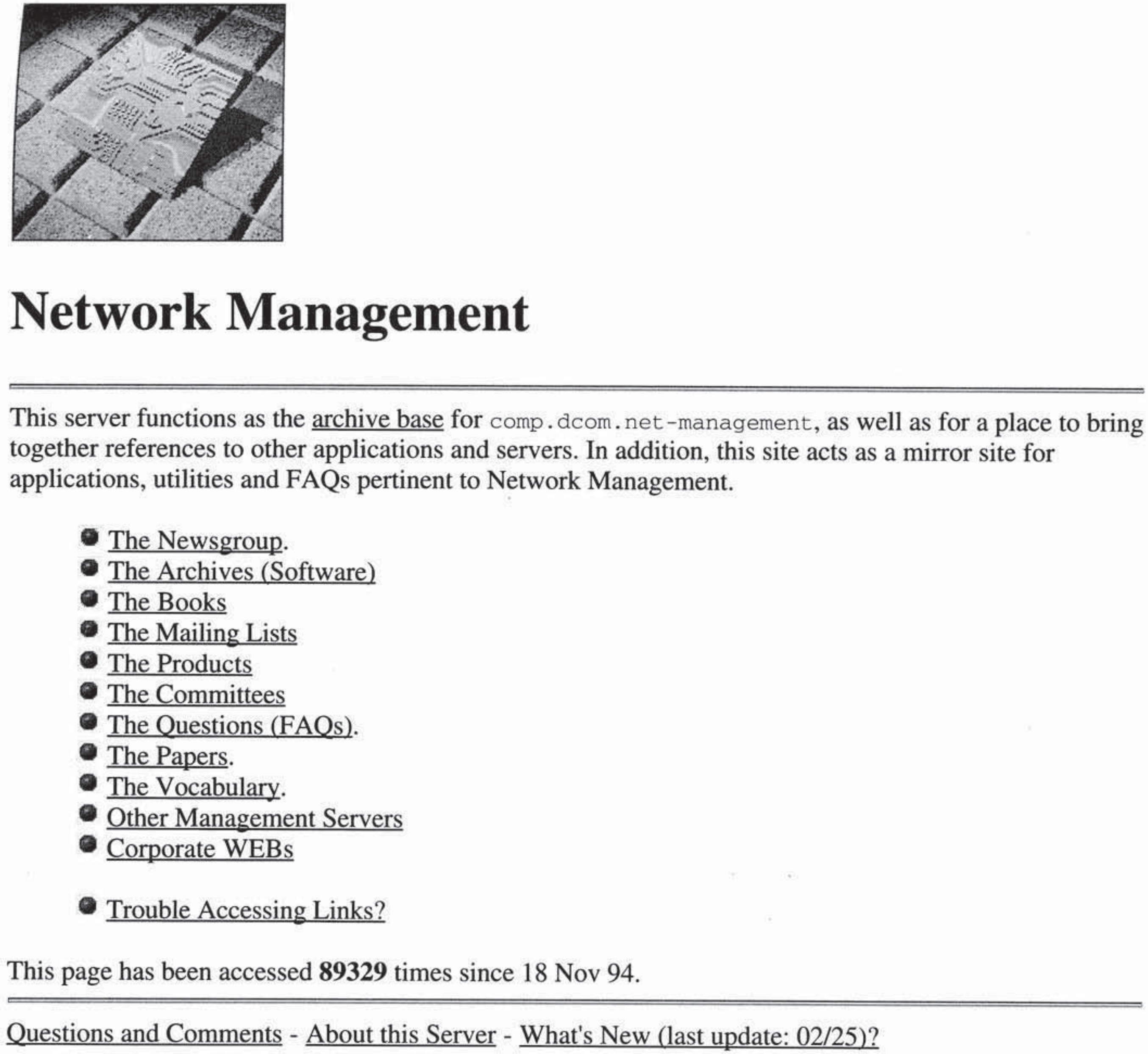
News groups that are relevant to the topic of this book include

- `comp.protocols.snmp`: Discusses topics related to SNMP
- `info.snmp`: a mirror of the SNMP mailing list
- `comp.dcom.net-management`: discusses network management topics

1A.3 Web Sites

The **World Wide Web** is the most convenient way of gathering information via the Internet. Useful Web sites for SNMP and network management include

- `http://smurfland.cit.buffalo.edu/NetMan/index.html`: a good overall site for information on network management topics. This site has links to many of the vendors who offer SNMP, RMON, and other network management products (Figure 1.6).
- `http://snmp.cs.utwente.nl/General/snmp.html`: known as "The Simple Web" site. It is a good source of information on SNMP, including pointers to many public-domain implementations (Figure 1.7).
- `http://www.nmf.org`: the home page for the Network Management Forum (NMF), a nonprofit organization whose members are vendors, customers, and others concerned with standardizing network management protocol and services. Although the original focus of the NMF was OSI network management, it has since expanded its charter to include the promotion of SNMP-based products and solutions (Figure 1.8).



Network Management

This server functions as the archive base for `comp.dcom.net-management`, as well as for a place to bring together references to other applications and servers. In addition, this site acts as a mirror site for applications, utilities and FAQs pertinent to Network Management.

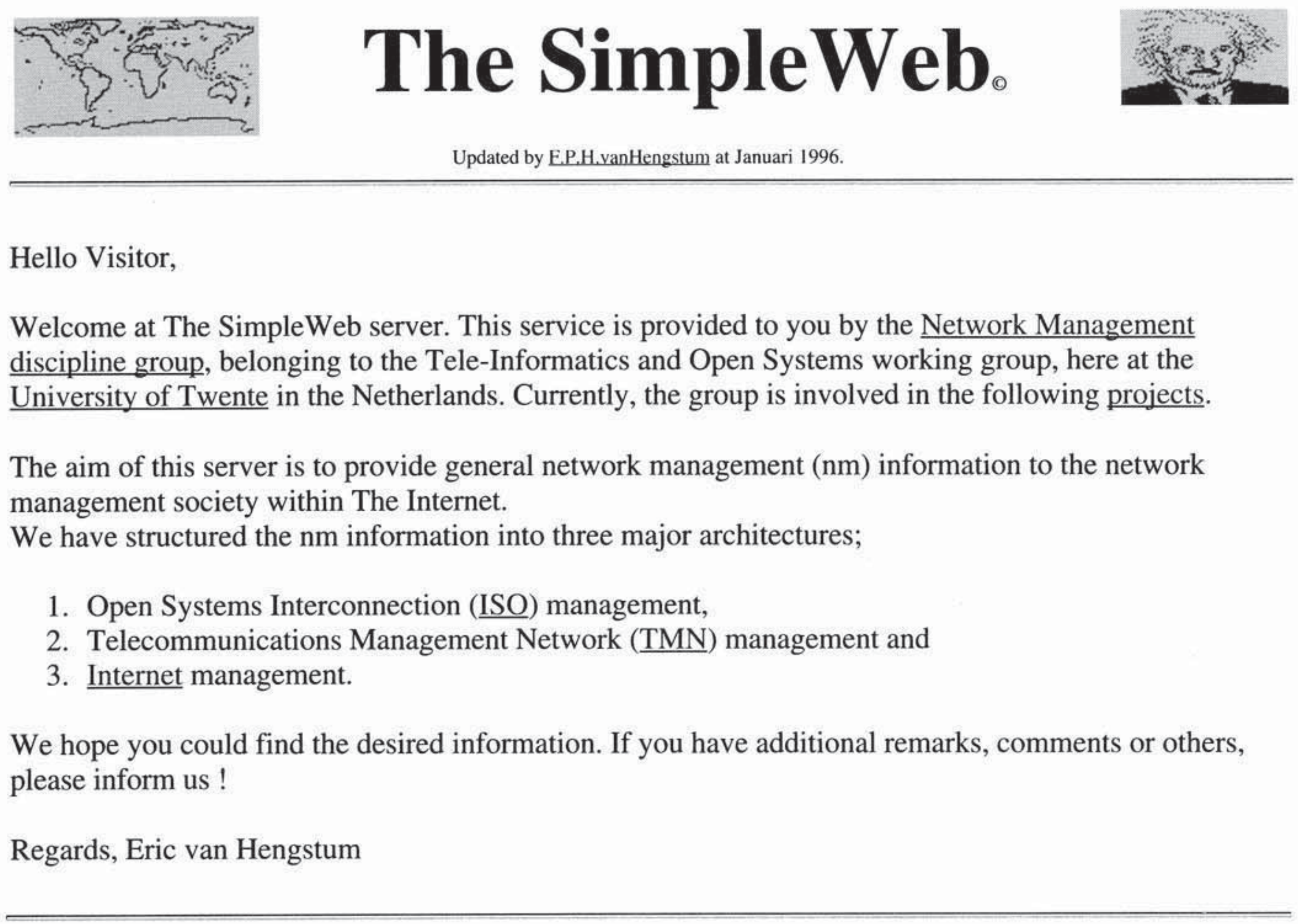
- The Newsgroup.
- The Archives (Software)
- The Books
- The Mailing Lists
- The Products
- The Committees
- The Questions (FAQs).
- The Papers.
- The Vocabulary.
- Other Management Servers
- Corporate WEBs

- Trouble Accessing Links?

This page has been accessed **89329** times since 18 Nov 94.

Questions and Comments - About this Server - What's New (last update: 02/25)?

FIGURE 1.6 Network Management Web Site
(`http://smurfland.cit.buffalo.edu /NetMan /index.html`)



The SimpleWeb©

Updated by F.P.H.vanHengstum at Januari 1996.

Hello Visitor,

Welcome at The SimpleWeb server. This service is provided to you by the Network Management discipline group, belonging to the Tele-Informatics and Open Systems working group, here at the University of Twente in the Netherlands. Currently, the group is involved in the following projects.

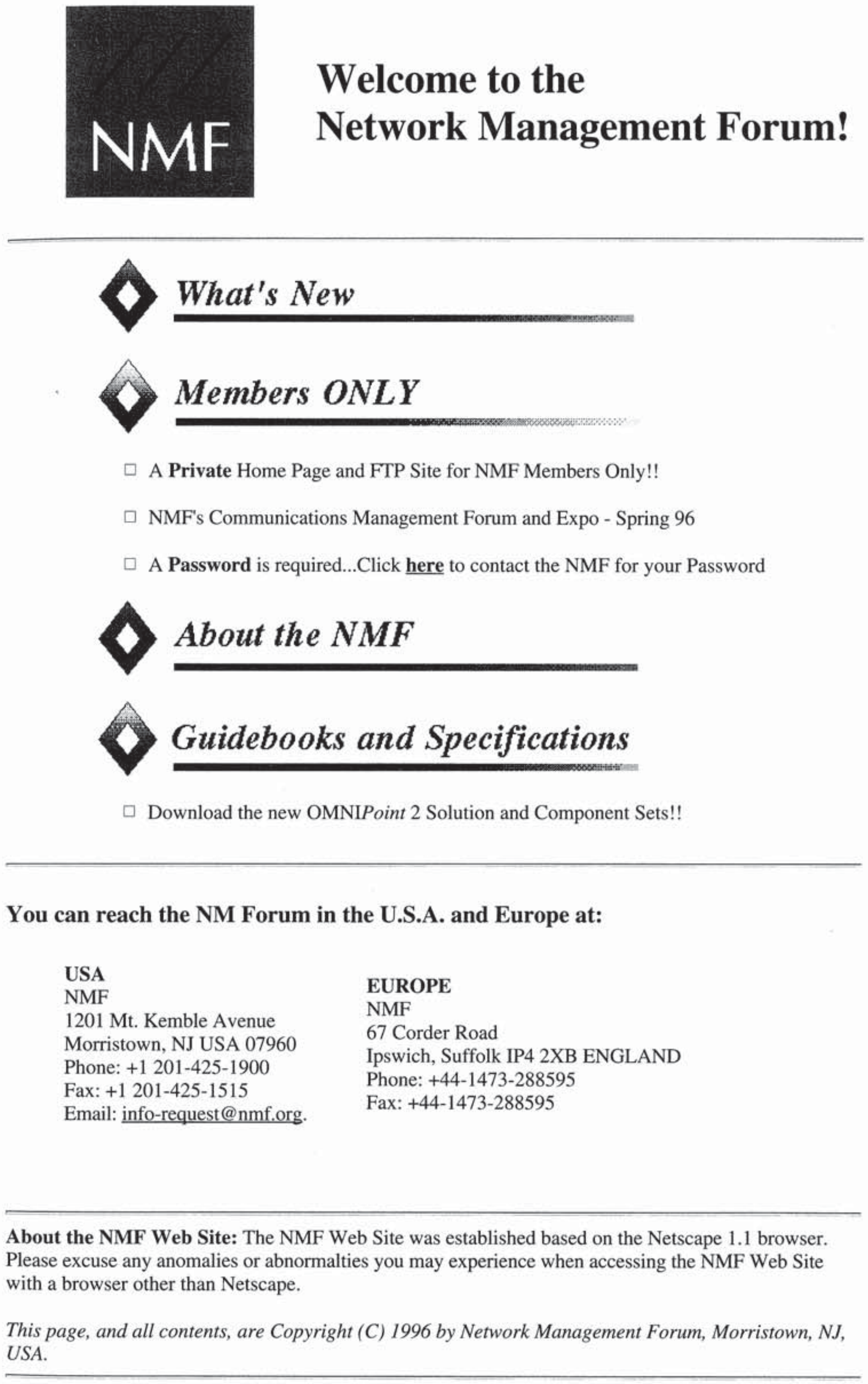
The aim of this server is to provide general network management (nm) information to the network management society within The Internet.
We have structured the nm information into three major architectures;

1. Open Systems Interconnection (ISO) management,
2. Telecommunications Management Network (TMN) management and
3. Internet management.

We hope you could find the desired information. If you have additional remarks, comments or others, please inform us !

Regards, Eric van Hengstum

FIGURE 1.7 The Simple Web (`http://snmp.cs.utwente.nlGeneral /snmp.html`)



NMF

Welcome to the Network Management Forum!

What's New

Members ONLY

□ A **Private** Home Page and FTP Site for NMF Members Only!!

□ NMF's Communications Management Forum and Expo - Spring 96

□ A **Password** is required...Click **here** to contact the NMF for your Password

About the NMF

Guidebooks and Specifications

□ Download the new OMNI*Point* 2 Solution and Component Sets!!

You can reach the NM Forum in the U.S.A. and Europe at:

USA
NMF
1201 Mt. Kemble Avenue
Morristown, NJ USA 07960
Phone: +1 201-425-1900
Fax: +1 201-425-1515
Email: info-request@nmf.org.

EUROPE
NMF
67 Corder Road
Ipswich, Suffolk IP4 2XB ENGLAND
Phone: +44-1473-288595
Fax: +44-1473-288595

About the NMF Web Site: The NMF Web Site was established based on the Netscape 1.1 browser. Please excuse any anomalies or abnormalties you may experience when accessing the NMF Web Site with a browser other than Netscape.

This page, and all contents, are Copyright (C) 1996 by Network Management Forum, Morristown, NJ, USA.

FIGURE 1.8 The Network Management Forum Web Site (`http://www.nmf.org`)

1A.4 Errata

As soon as any typos or other errors are discovered, an errata list for this book will be available at my web site at `http://www.shore.net/~ws/welcome.html`. The file will be updated as needed. Please send any errors that you spot to me at `ws@shore.net`.

Errata sheets for all of my other books are at the same web site, as well as a discount order form for the books.

Notes

1. *Source:* International Data Corp., May 1992.
2. In this chapter, the term *user* refers to the user of a network management system or application. The user of the network, computers, and other applications as a whole is referred to as an *end user*.

PART ONE

Network Management Fundamentals

CHAPTER 2

Network Monitoring

The network-monitoring portion of network management is concerned with observing and analyzing the status and behavior of the end systems, intermediate systems, and subnetworks that make up the configuration to be managed.

(Chiu and Sudama 1992) suggest that network monitoring consists of three major design areas:

- *access to monitored information:* how to define monitoring information, and how to get that information from a resource to a manager
- *design of monitoring mechanisms:* how best to obtain information from resources
- *application of monitored information:* how the monitored information is used in various management functional areas

The first section in this chapter deals with the first two items in the preceding list, by examining some of the general design considerations for a network-monitoring system. The remainder of the chapter deals with network-monitoring applications. Network monitoring encompasses all five of the functional areas listed in Table 1.1. In this chapter we focus on the three functional areas that generally are most important for network monitoring: performance monitoring, fault monitoring, and accounting monitoring.

2.1 Network-Monitoring Architecture

Before considering the design of a network-monitoring system, it is best to consider the type of information that is of interest to a network monitor. Then we can look at the alternatives for configuring the network-monitoring function.

2.1.1 Network-Monitoring Information

The information that should be available for network monitoring can be classified as follows:

- *static:* This is information that characterizes the current configuration and the elements in the current configuration, such as the number and identification of ports on a router. This information will change only infrequently.

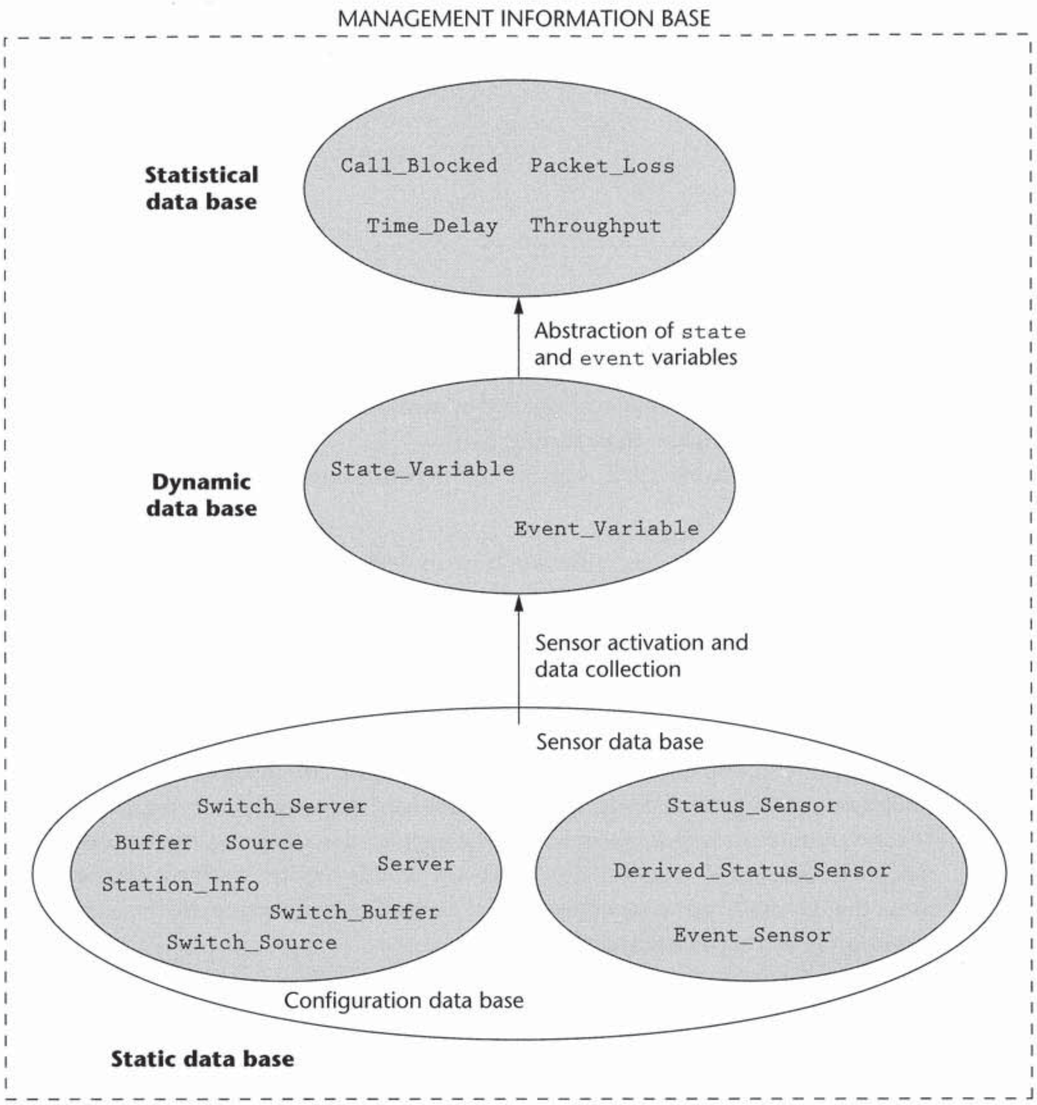


FIGURE 2.1 **Organization of a Management Information Base**

- *dynamic:* This information is related to events in the network, such as a change of state of a protocol machine or the transmission of a packet on a network.
- *statistical:* This is information that may be derived from dynamic information, such as the average number of packets transmitted per unit time by an end system.

An example of such an information structure, for use in monitoring a real-time system, is suggested in (Mazumdar and Lazar 1991). In this scheme, the static data base has two major components: a configuration data base with basic information about the computer and networking elements, and a sensor data base, with information about sensors used to obtain real-time readings. The dynamic data base is primarily concerned with collecting information about the state of various network elements and events detected by the sensors. The statistical data base includes useful aggregate measures. Figure 2.1 suggests the relationships among these components.

The nature of the monitored information has implications for where it is collected and stored for purposes of monitoring. Static information is typically generated by the element involved. Thus, a router maintains its own configuration information. This information can be made available directly to a monitor if the element has the appropriate agent software. Alternatively, the information can be made available to a proxy that in turn will make it available to a monitor.

Dynamic information, too, is generally collected and stored by the network element responsible for the underlying events. However, if a system is attached to a LAN, then much of its activity can be observed by another system on the LAN. The term "remote monitor" refers to a device on a LAN that observes all of the traffic on the LAN and gathers information about that traffic. For example, the total number of packets issued by an element on a LAN could be recorded by the element itself or by a remote monitor that is listening on the same LAN. Some dynamic information, however, can be generated only by the element itself, such as the current number of network-level connections.

Statistical information can be generated by any system that has access to the underlying dynamic information. The statistical information could be generated back at the network monitor itself. This would require that all of the "raw" data be transmitted to the monitor, where it would be analyzed and summarized. If the monitor does not need access to all of the raw data, then monitor processing time and network capacity could be saved if the system that holds the dynamic data does the summarization and sends the results to the monitor.

2.1.2 Network-Monitoring Configurations

Figure 2.2, based on a depiction in (Chiu and Sudama 1992), illustrates the architecture for network monitoring in functional terms. Part (a) of the figure shows the four major components of a network-monitoring system:

- *monitoring application:* This component includes the functions of network monitoring that are visible to the user, such as performance monitoring, fault monitoring, and accounting monitoring.
- *manager function:* This is the module at the network monitor that performs the basic monitoring function of retrieving information from other elements of the configuration.
- *agent function:* This module gathers and records management information for one or more network elements and communicates the information to the monitor.
- *managed objects:* This is the management information that represents resources and their activities.

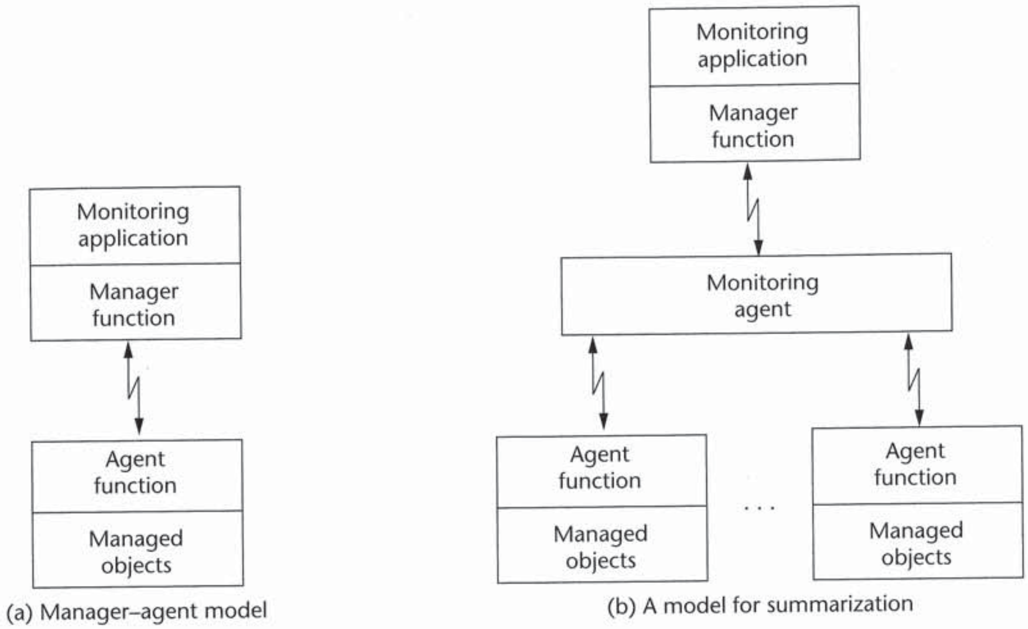


FIGURE 2.2 **Functional Architecture for Network Monitoring**

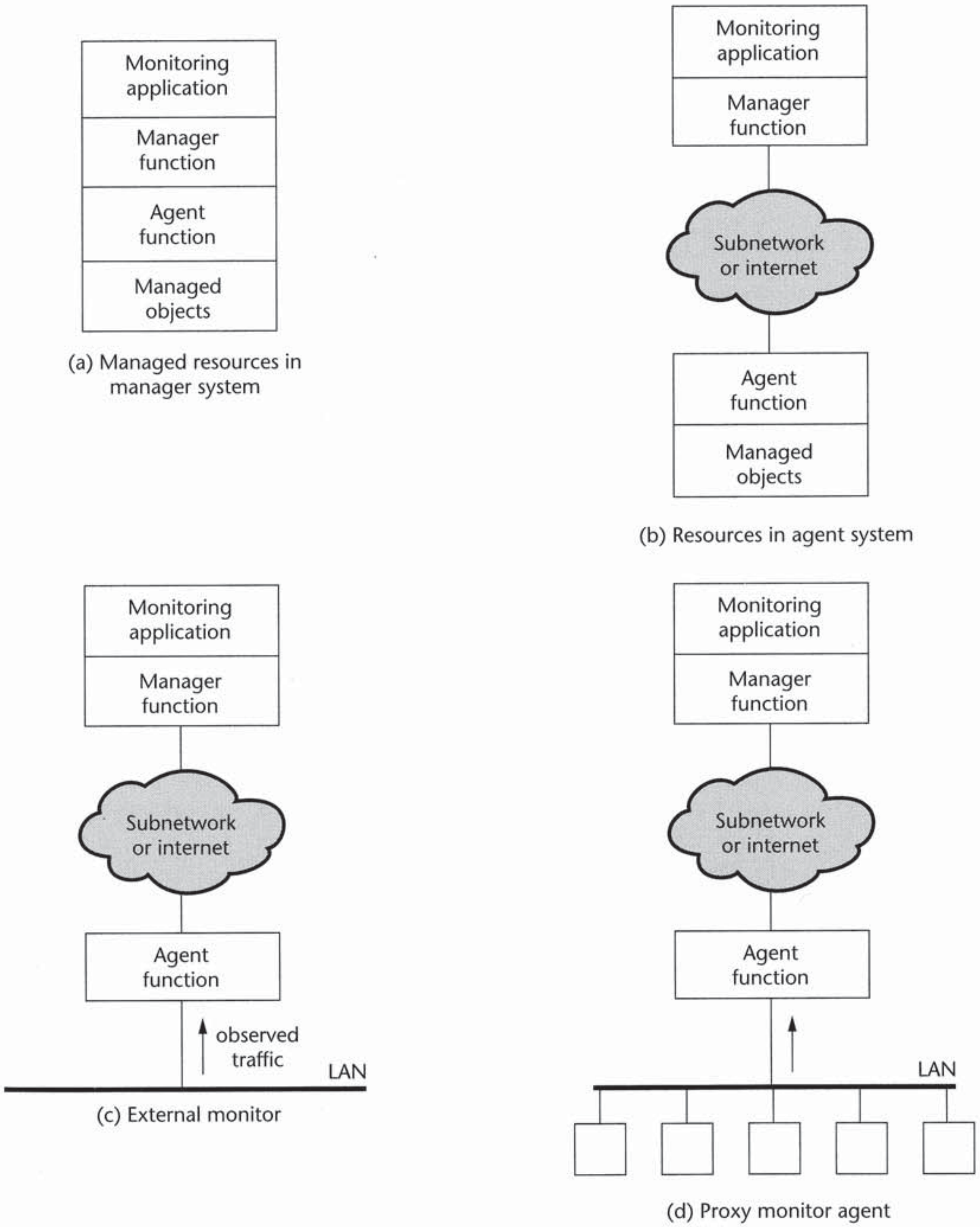
It is useful to highlight an additional functional module concerned with statistical information (Figure 2.2, part (b)):

- *Monitoring agent:* This module generates summaries and statistical analyses of management information. If remote from the manager, this module acts as an agent and communicates the summarization information to the manager.

These functional modules may be configured in a number of ways. The station that hosts the monitoring application is itself a network element and subject to monitoring. Thus, the network monitor generally includes agent software and a set of managed objects (Figure 2.3 (a)). In fact, it is vital to monitor the status and behavior of the network monitor to assure that it continues to perform its function and to assess the load on itself and on the network. One key requirement is that the network management protocol be instrumented to monitor the amount of network management traffic into and out of the network monitor.

Figure 2.3 (b) illustrates the most common configuration for monitoring other network elements. This configuration requires that the manager and agent systems share the same network management protocol and MIB (management information base) syntax and semantics.

A network-monitoring system may also include one or more agents that monitor traffic on



(a) Managed resources in manager system

(b) Resources in agent system

(c) External monitor

(d) Proxy monitor agent

FIGURE 2.3 **Network-Monitoring Configurations**

a network. These are often referred to as external monitors or remote monitors; the configuration is depicted in Figure 2.3 (c).

Finally, as was discussed in Section 1.2.4, for network elements that do not share a common network management protocol with the network monitor, a proxy agent is needed (Figure 2.3 (d)).

2.1.3 Polling and Event Reporting

Information that is useful for network monitoring is collected and stored by agents and made available to one or more manager systems. Two techniques are used to make the agent information available to the manager: polling and event reporting.

Polling is a request–response interaction between a manager and agent. The manager can query any agent (for which it has authorization) and request the values of various information elements; the agent responds with information from its MIB. The request may be specific, listing one or more named variables. A request may also be in the nature of a search, asking the agent to report information matching certain criteria, or to supply the manager with information about the structure of the MIB at the agent. A manager system may use polling to learn about the configuration it is managing, to obtain periodically an update of conditions, or to investigate an area in detail after being alerted to a problem. Polling is also used to generate a report on behalf of a user and to respond to specific user queries.

With **event reporting,** the initiative is with the agent and the manager is in the role of a listener, waiting for incoming information. An agent may generate a report periodically to give the manager its current status. The reporting period may be preconfigured or set by the manager. An agent may also generate a report when a significant event (e.g., a change of state) or an unusual event (e.g., a fault) occurs. Event reporting is useful for detecting problems as soon as they occur. It is also more efficient than polling for monitoring objects whose states or values change relatively infrequently.

Both polling and event reporting are useful, and a network-monitoring system will typically employ both methods. The relative emphasis placed on the two methods varies greatly in different systems. Telecommunications management systems have traditionally placed a very high reliance on event reporting. In contrast, the SNMP approach puts very little reliance on event reporting. OSI systems management tends to fall somewhere between these extremes. However, both SNMP and OSI systems management, as well as most proprietary schemes, allow the user considerable latitude in determining the relative emphasis on the two approaches. The choice of emphasis depends on a number of factors, including the following:

- the amount of network traffic generated by each method
- robustness in critical situations
- the time delay in notifying the network manager
- the amount of processing in managed devices

- the tradeoffs of reliable versus unreliable transfer
- the network-monitoring applications being supported
- the contingencies required in case a notifying device fails before sending a report

2.2 *Performance Monitoring*

2.2.1 Performance Indicators

An absolute prerequisite for the management of a communications network is the ability to measure the performance of the network, or **performance monitoring.** We cannot hope to manage and control a system or activity unless we can monitor its performance. One of the difficulties facing the network manager is in the selection and use of the appropriate indicators that measure the network's performance. Among the problems that may appear are the following:

- There are too many indicators in use.
- The meanings of most indicators are not yet clearly understood.
- Some indicators are introduced and supported by some manufacturers only.
- Most indicators are not suitable for comparison with each other.
- Frequently, the indicators are accurately measured but incorrectly interpreted.
- In many cases, the calculation of indicators takes too much time, and the final results can hardly be used for controlling the environment.

In this section, we give some general ideas of the types of indicators that are useful for network management. These fall into two categories: service-oriented measures and efficiency-oriented measures; Table 2.1, based on (Terplan 1992), gives a breakdown of major indicators in each category. The principal means of judging that a network is meeting its requirements is that specified service levels are maintained to the satisfaction of the users. Thus, service-oriented indicators are of the highest priority. The manager is also concerned with meeting these requirements at minimum cost, hence the need for efficiency-oriented measures.

2.2.1.1 Availability

Availability can be expressed as the percentage of time that a network system, component, or application is available for a user. Depending on the application, high availability can be significant. For example, in an airline reservation network, a one-minute outage may cause $10,000 in losses; in a banking network, a one-hour outage may introduce losses in the millions of dollars.

Availability is based on the reliability of the individual components of a network. Reliability is the probability that a component will perform its specified function for a specified time under

TABLE 4.1 *Continued*

RFC	Date	Title
		PROPOSED STANDARDS
1239	June 1991	Reassignment of Experimental MIBs to Standard MIBs
1253	August 1991	OSPF Version 2 Management Information Base
1315	April 1992	Management Information Base for Frame Relay DTEs
1354	July 1992	IP Forwarding Table MIB
1381	November 1992	SNMP MIB Extension for X.25 LAPB
1382	November 1992	SNMP MIB Extension for the X.25 Packet Layer
1406	January 1993	DS1 Interface Type MIB
1407	January 1993	DS3 Interface Type MIB
1414	February 1993	Identification MIB
1418	March 1993	SNMP over OSI
1419	March 1993	SNMP over AppleTalk
1420	March 1993	SNMP over IPX
1461	May 1993	SNMP MIB Extension for Multiprotocol Interconnect over X.25
1471	June 1993	Definitions of Managed Objects for the Link Control Protocol of PPP
1472	June 1993	Definitions of Managed Objects for the Security Protocols of PPP
1473	June 1993	Definitions of Managed Objects for the IP Network Control Protocol of PPP
1474	June 1993	Definitions of Managed Objects for Bridge Network Control Protocol of PPP
1512	September 1993	FDDI MIB
1514	September 1993	Host Resources MIB
1515	September 1993	Definitions of Managed Objects for IEEE 802.3 MAUs
1525	September 1993	Definitions of Managed Objects for Source Routing Bridges
1565	January 1994	Network Services Monitoring MIB
1566	January 1994	Mail Monitoring MIB
1567	January 1994	X.500 Directory Monitoring MIB
1573	January 1994	Extensions to the Generic-Interface MIB
1595	March 1994	Definitions of Managed Objects for the SONET/SDH Interface Type
1604	March 1994	Definitions of Managed Objects for Frame Relay Service
1611	March 1994	DNS Server MIB Extensions
1612	March 1994	DNS Resolver MIB Extensions
1628	March 1994	UPS MIB
1665	July 1994	Definitions of Managed Objects for SNA NAUs
1695	August 1994	Definitions of Managed Objects for ATM Management Version 8.0
1696	August 1994	Modem MIB
1697	August 1994	Relational Database Management System MIB
1742	January 1995	Appletalk MIB
1747	January 1995	SDLC MIB
1749	December 1994	IEEE 802.5 MIB
1759	March 1995	Printer MIB
		INFORMATIONAL
1215	March 1991	A Convention for Defining Traps for Use with the SNMP

- Management Information Base for Network Management of TCP/IP-based Internets: MIB-II (RFC 1213): describes the managed objects contained in the MIB
- Simple Network Management Protocol (RFC 1157): defines the protocol used to manage these objects

The remaining RFCs listed in Table 4.1 define various extensions to the SMI or MIB.

4.2 *Basic Concepts*

4.2.1 Network Management Architecture

The model of network management that is used for TCP/IP network management includes the following key elements:

- management station
- management agent
- management information base
- network management protocol

The **management station** is typically a stand-alone device, but it may be a capability implemented on a shared system. In either case, the management station serves as the interface for the human network manager into the network management system. At a minimum, the management station will have

- a set of management applications for data analysis, fault recovery, and so on
- an interface by which the network manager may monitor and control the network
- the capability of translating the network manager's requirements into the actual monitoring and control of remote elements in the network
- a data base of information extracted from the MIBs of all the managed entities in the network

Only the last two elements are the subject of SNMP standardization.

The other active element in the network management system is the **management agent**. Key platforms, such as hosts, bridges, routers, and hubs, may be equipped with SNMP agents so that they may be managed from a management station. The management agent responds to requests for information and actions from the management station and may asynchronously provide the management station with important but unsolicited information.

Resources in the network may be managed by representing these resources as objects. Each object is, essentially, a data variable that represents one aspect of the managed agent. The collection of objects is referred to as a **management information base** (**MIB**). The MIB functions as a collection of access points at the agent for the management station. These objects are standardized across systems of a particular class (e.g., a common set of objects is used for the management of various bridges). A management station performs the monitoring function by retrieving the value of MIB objects. A management station can cause an action to take place at an agent or can change the configuration settings at an agent by modifying the value of specific variables.

The management station and agents are linked by a **network management protocol**. The protocol used for the management of TCP/IP networks is the Simple Network Management Protocol (SNMP), which includes the following key capabilities:

- `get`: enables the management station to retrieve the value of objects at the agent
- `set`: enables the management station to set the value of objects at the agent
- `trap`: enables an agent to notify the management station of significant events

The standards do not specify the number of management stations or the ratio of management stations to agents. In general, it is prudent to have at least two systems capable of performing the management station function, to provide redundancy in case of failure. The other issue is the practical one of how many agents a single management station can handle. As long as SNMP remains relatively "simple," that number can be quite high, certainly in the hundreds.

4.2.2 Network Management Protocol Architecture

SNMP was designed to be an application-level protocol that is part of the TCP/IP protocol suite. It is intended to operate over the User Datagram Protocol (UDP).[2] Figure 4.1 suggests the typical configuration of protocols for SNMP. For a stand-alone management station, a manager process controls access to a central MIB at the management station and provides an interface to the network manager. The manager process achieves network management by using SNMP, which is implemented on top of UDP, IP, and the relevant network-dependent protocols (e.g., Ethernet, FDDI, and X.25).

Each agent must also implement SNMP, UDP, and IP. In addition, an agent process interprets the SNMP messages and controls the agent's MIB. For an agent device that supports other applications, such as FTP, both TCP and UDP are required. The shaded portions in the figure depict the operational environment—that which is to be managed. The unshaded portions provide support to the network management function.

Figure 4.2 provides a somewhat closer look at the protocol context of SNMP. From a management station, three types of SNMP messages are issued on behalf of a management application: `GetRequest`, `GetNextRequest`, and `SetRequest`. The first two are two variations of the `get` function. All three messages are acknowledged by the agent in the form of a `GetResponse` message, which is passed up to the management application. In addition, an agent may issue a trap message in response to an event that affects the MIB and the underlying managed resources.

Because SNMP relies on UDP, which is a connectionless protocol, SNMP is itself con-

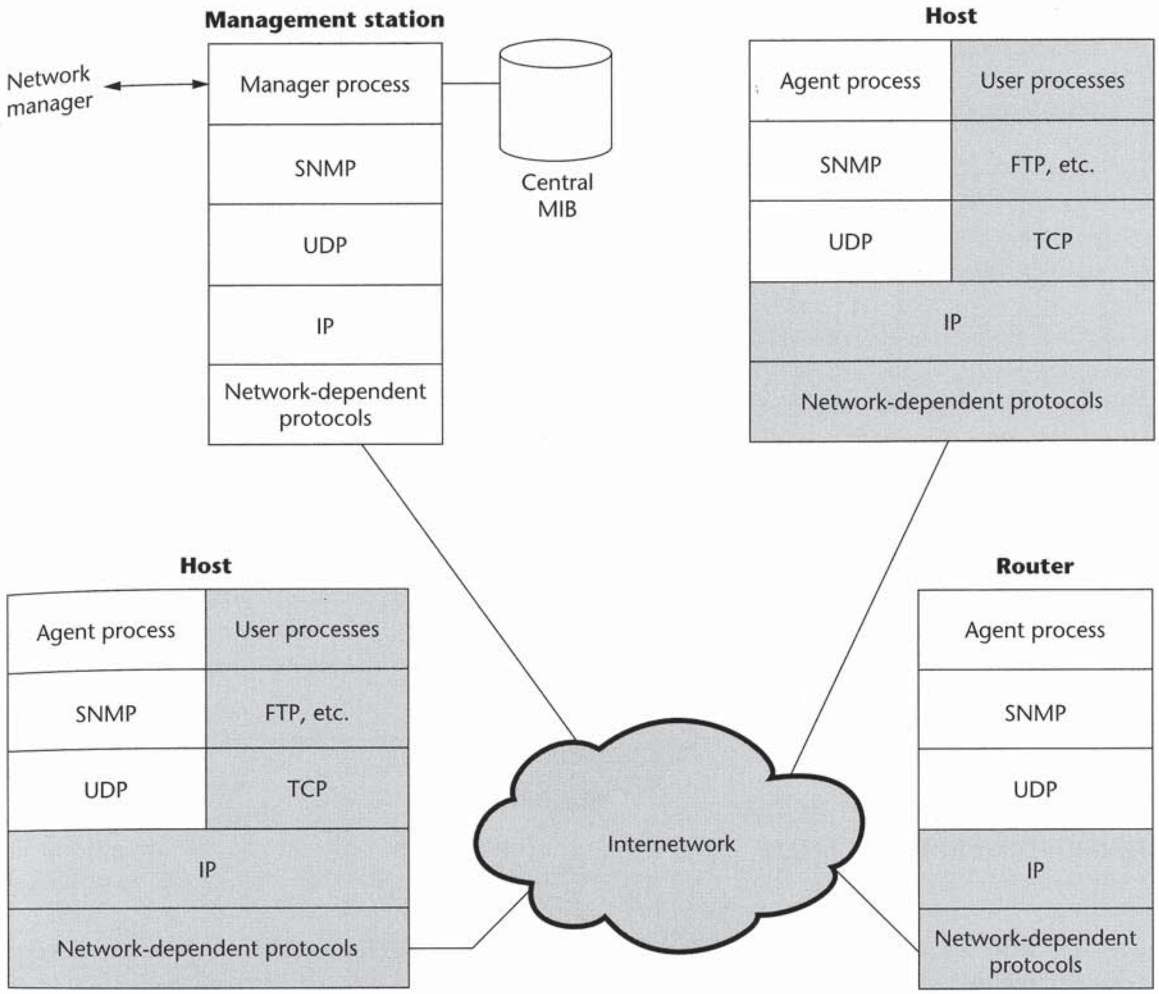


FIGURE 4.1 **Configuration of SNMP**

nectionless. No ongoing connections are maintained between a management station and its agents. Instead, each exchange is a separate transaction between a management station and an agent.

4.2.3 Trap-directed Polling

If a management station is responsible for a large number of agents, and if each agent maintains a large number of objects, then it becomes impractical for the management station regularly to poll all agents for all of their readable object data. Instead, SNMP and the associated

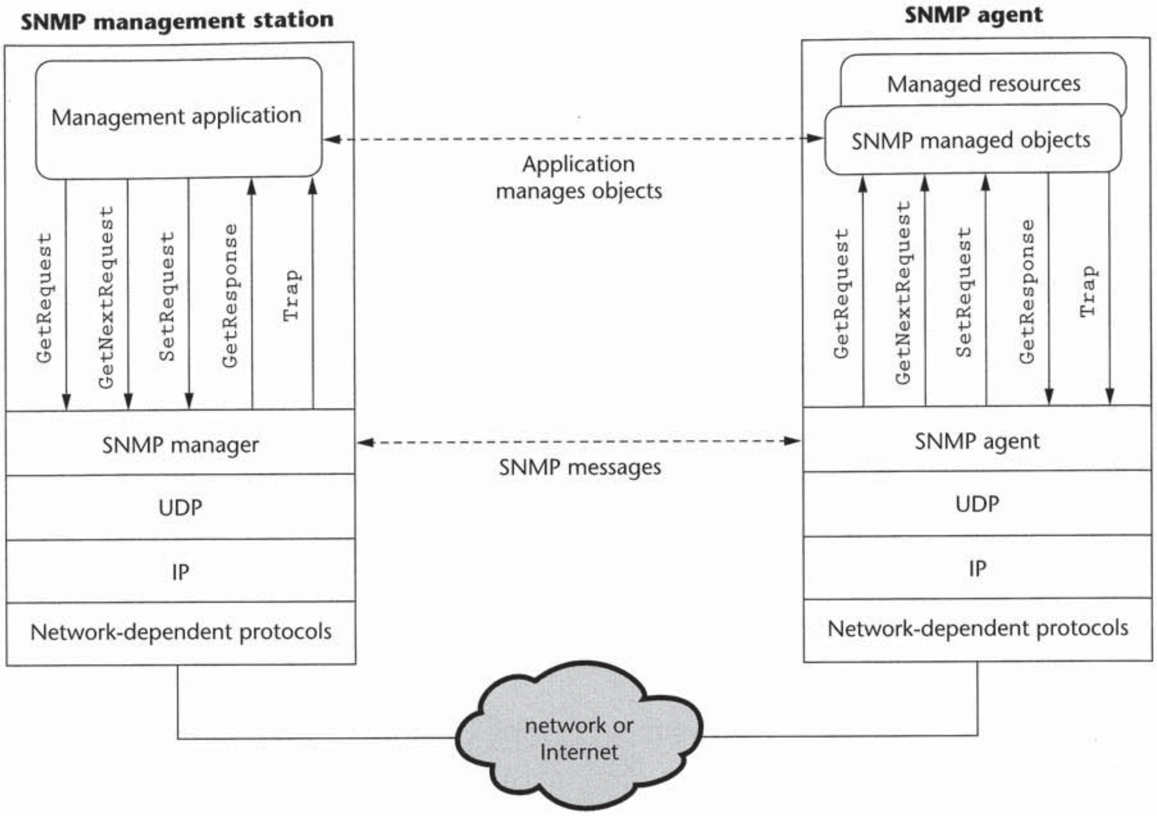


FIGURE 4.2 The Role of SNMP

MIB are designed to encourage the manager to use a technique referred to as **trap-directed polling.**

The preferred strategy is this. At initialization time, and perhaps at infrequent intervals, such as once a day, a management station can poll all of the agents it knows for some key information, such as interface characteristics and perhaps some baseline performance statistics, such as the average number of packets sent and received over each interface over a given period of time. Once this baseline is established, the management station refrains from polling. Instead, each agent is responsible for notifying the management station of any unusual event; for example, the agent crashes and is rebooted, a link fails, or an overload condition as defined by the packet load crosses some threshold. These events are communicated in SNMP messages known as traps.

Once a management station is alerted to an exception condition, it may choose to take some action. At this point, the management station may direct polls to the agent reporting the event and perhaps to some nearby agents in order to diagnose any problem and to gain more specific information about the exception condition.

Trap-directed polling can result in substantial savings of network capacity and agent processing time. In essence, the network is not made to carry management information that the management station does not need, and agents are not made to respond to frequent requests for uninteresting information.

4.2.4 Proxies

The use of SNMP requires that all agents, as well as management stations, must support a common protocol suite, such as UDP and IP. This limits direct management to such devices and excludes other devices, such as some bridges and modems, that do not support any part of the TCP/IP protocol suite. Further, there may be numerous small systems (personal computers, workstations, programmable controllers) that do implement TCP/IP to support their applications, but for which it is not desirable to add the additional burden of SNMP, agent logic, and MIB maintenance.

To accommodate devices that do not implement SNMP, the concept of proxy was developed. In this scheme an SNMP agent acts as a proxy for one or more other devices; that is, the SNMP agent acts on behalf of the proxied devices.

Figure 4.3 indicates the type of protocol architecture that is often involved. The management

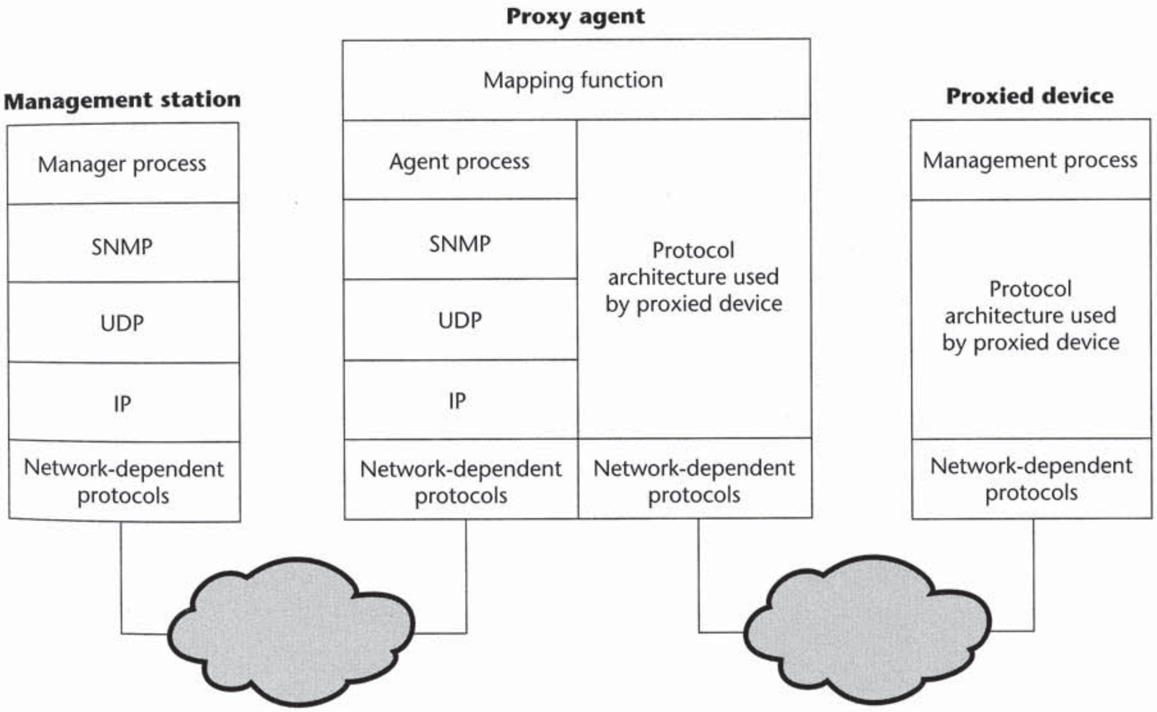

Proxy agent
Mapping function
Management station
Proxied device
Manager process
SNMP
UDP
IP
Network-dependent protocols
Agent process
SNMP
UDP
IP
Network-dependent protocols
Protocol architecture used by proxied device
Network-dependent protocols
Management process
Protocol architecture used by proxied device
Network-dependent protocols

FIGURE 4.3 Proxy Configuration

station sends queries concerning a device to its proxy agent. The proxy agent converts each query into the management protocol that the device is using. When the agent receives a reply to a query, it passes that reply back to the management station. Similarly, if an event notification of some sort from the device is transmitted to the proxy, the proxy sends that on to the management station in the form of a trap message.

4.3 *Summary*

The Simple Network Management Protocol was designed to be an easily implemented, basic network management tool that could be used to meet short-term network management needs. Because of the slow progress in OSI systems management, SNMP has filled the gap and become the dominant standardized network management scheme in use today.

The SNMP set of standards provides a framework for the definition of management information and a protocol for the exchange of that information. The SNMP model assumes the existence of managers and agents. A manager is a software module in a management system responsible for managing part or all of the configuration on behalf of network management applications and users. An agent is a software module in a managed device responsible for maintaining local management information and delivering that information to a manager via SNMP. A management information exchange can be initiated by the manager (via polling) or by the agent (via a trap).

SNMP accommodates the management of devices that do not implement the SNMP software by means of proxies. A proxy is an SNMP agent that maintains information on behalf of one or more non-SNMP devices.

Notes

1. See Appendix A for a brief technical discussion of TCP/IP. A more detailed discussion can be found in (Stallings 1996c).
2. See Appendix A for a brief description of UDP.

CHAPTER 5

SNMP Management Information

As with any network management system, the foundation of a TCP/IP-based network management system is a data base containing information about the elements to be managed. In both the TCP/IP and the OSI environments, the data base is referred to as a management information base (MIB). Each resource to be managed is represented by an object. The MIB is a structured collection of such objects. For SNMP, the MIB is, in essence, a database structure in the form of a tree. Each system (workstation, server, router, bridge, etc.) in a network or internetwork maintains a MIB that reflects the status of the managed resources at that system. A network management entity can monitor the resources at that system by reading the values of objects in the MIB and may control the resources at that system by modifying those values.

In order for the MIB to serve the needs of a network management system, it must meet certain objectives:

1. *The object or objects used to represent a particular resource must be the same at each system.* For example, consider information stored concerning the TCP entity at a system. The total number of connections opened over a period of time consists of active opens and passive opens. The MIB at the system could store any two of the three relevant values (number of active opens, number of passive opens, total number of opens), from which the third could be derived when needed. However, if different systems select different pairs for storage, it is difficult to write a simple protocol to access the required information. As it happens, the MIB definition for TCP/IP specifies that the active and passive open counts be stored.
2. *A common scheme for representation must be used to support interoperability.*

The second point is addressed by defining a structure of management information (SMI), which we examine in this chapter, together with a look at some of the practical issues involved in managing by means of managed objects. The first point is addressed by defining the objects and the structuring of those objects in the MIB; Chapter 6 looks at some important examples.

This chapter makes use of the ASN.1 notation. The reader not familiar with this notation should first consult Appendix B.

7.1.2 Communities and Community Names

Network management can be viewed as a distributed application. Like other distributed applications, network management involves the interaction of a number of application entities supported by an application protocol. In the case of SNMP network management, the application entities are the management station applications and the managed station (agent) applications that use SNMP, which is the supporting protocol.

SNMP network management has several characteristics not typical of all distributed applications. The application involves a one-to-many relationship between a management station and a set of managed stations: The management station is able to get and set objects in the managed stations and is able to receive traps from the managed stations. Thus, from an operational or control point of view, the management station "manages" a number of managed stations. There may be a number of management stations, each of which manages all or a subset of the managed stations in the configuration. These subsets may overlap.

Interestingly, we also need to be able to view SNMP network management as a one-to-many relationship between a managed station and a set of management stations. Each managed station controls its own local MIB and must be able to control the use of that MIB by a number of management stations. There are three aspects to this control:

- *authentication service:* The managed station may wish to limit access to the MIB to authorized managed stations.
- *access policy:* The managed station may wish to give different access privileges to different management stations.
- *proxy service:* A managed station may act as a proxy to other managed stations. This may involve implementing the authentication service and/or access policy for the other managed systems on the proxy system.

All of these aspects relate to security concerns. In an environment in which responsibility for network components is split, such as among a number of administrative entities, managed systems need to protect themselves and their MIBs from unwanted and unauthorized access. SNMP, as defined in RFC 1157, provides only a primitive and limited capability for such security, namely the concept of a community.

An **SNMP community** is a relationship between an SNMP agent and a set of SNMP managers that defines authentication, access control, and proxy characteristics. The community concept is a local one, defined at the managed system. The managed system establishes one community for each desired combination of authentication, access control, and proxy characteristics. Each community is given a unique (within this agent) community name, and the management stations within that community are provided with and must employ the community name in all get and set operations. The agent may establish a number of communities, with overlapping management station membership.

Since communities are defined locally at the agent, the same name may be used by different agents. This identity of names is irrelevant and does not indicate any similarity between the defined communities. Thus, a management station must keep track of the community name or names associated with each of the agents that it wishes to access.

7.1.2.1 Authentication Service

An authentication service is concerned with ensuring that a communication is authentic. In the case of an SNMP message, the function of an authentication service would be to assure the recipient that the message is from the source from which it claims to be. As defined in RFC 1157, SNMP provides for only a trivial scheme for authentication. Every message (get or put request) from a management station to an agent includes a community name. This name functions as a password, and the message is assumed to be authentic if the sender knows the password.

With this limited form of authentication, many network managers will be reluctant to allow anything other than network monitoring; that is, `Get` and `Trap` operations. Network control, via a `Set` operation, is clearly a more sensitive area. The community name could be used to trigger an authentication procedure, with the name functioning simply as an initial password-screening device. The authentication procedure could involve the use of encryption/decryption for more secure authentication functions. This is beyond the scope of RFC 1157.

7.1.2.2 Access Policy

By defining a community, an agent limits access to its MIB to a selected set of management stations. By the use of more than one community, the agent can provide different categories of MIB access to different management stations. There are two aspects to this access control:

- *SNMP MIB view:* a subset of the objects within a MIB. Different MIB views may be defined for each community. The set of objects in a view need not belong to a single subtree of the MIB.
- *SNMP access mode:* an element of the set `{READ-ONLY, READ-WRITE}`. An access mode is defined for each community.

The combination of a MIB view and an access mode is referred to as an **SNMP community profile.** Thus, a community profile consists of a defined subset of the MIB at the agent, plus an access mode for those objects. The SNMP access mode is applied uniformly to all objects in the MIB view. Thus, if the access mode `READ-ONLY` is selected, it applies to all objects in the view and limits management stations' access to this view to read-only operations.

Within a community profile, two separate access restrictions must be reconciled. Recall that the definition of each MIB object includes an `ACCESS` clause (Figure 5.2). Table 7.1 shows the rules for reconciling an object's `ACCESS` clause with the SNMP access mode imposed for a particular view. Most of the rules are straightforward. Note, however, that even if an object is declared as write-only, it may be possible with SNMP to read that object; this is an implementation-specific matter.

TABLE 7.1 **Relationship Between MIB `ACCESS` Category and SNMP Access Mode**

MIB `ACCESS` Category	SNMP Access Mode	
	`READ-ONLY`	`READ-WRITE`
read-only	Available for get and trap operations	
read-write	Available for get and trap operations	Available for get, set, and trap operations
write-only	Available for get and trap operations, but the value is implementation-specific	Available for get, set, and trap operations, but the value is implementation-specific for get and trap operations
not accessible	Unavailable	

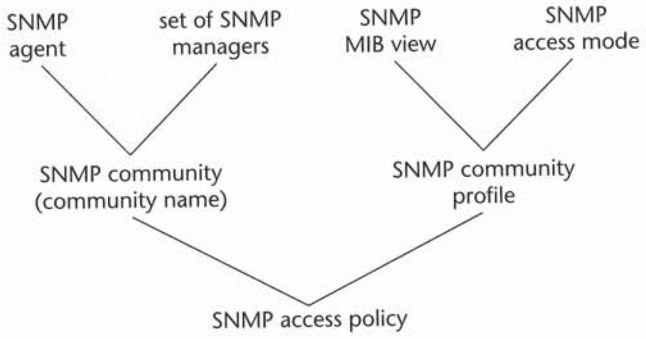


FIGURE 7.1 **Administrative Concepts**

A community profile is associated with each community defined by an agent; the combination of an SNMP community and an SNMP community profile is referred to as an **SNMP access policy**. Figure 7.1 illustrates the various concepts just introduced.

7.1.2.3 Proxy Service

The community concept is also useful in supporting the proxy service. Recall from Chapter 4 that a proxy is an SNMP agent that acts on behalf of other devices. Typically, the other devices are foreign, in that they do not support TCP/IP and SNMP. In some cases, the proxied system may support SNMP but the proxy is used to minimize the interaction between the proxied device and network management systems.

For each device that the proxy system represents, it maintains an SNMP access policy. Thus, the proxy knows which MIB objects can be used to manage the proxied system (the MIB view) and their access mode.

7.1.3 Instance Identification

We have seen that every object in a MIB has a unique object identifier, which is defined by the position of the object in the tree-structured MIB. However, when an access is made to a MIB, via SNMP or some other means, it is a specific instance of an object that is wanted, not an object type.

7.1.3.1 Columnar Objects

For objects that appear in tables, which we refer to as *columnar objects,* the object identifier alone does not suffice to identify the instance: There is one instance of each object for every row in the table. Therefore, some convention is needed by which a specific instance of an object within a table may be identified. In the SMI document (RFC 1155), it states that

> *The means whereby object instances are referenced is not defined in the MIB. Reference to object instances is achieved by a protocol-specific mechanism. It is the responsibility of each management protocol adhering to the SMI to define this mechanism.*

Thus we must turn to the SNMP document for the referencing convention. SNMP actually defines two techniques for identifying a specific object instance: a serial-access technique and a random-access technique. The serial-access technique is based on a lexicographic ordering of objects in the MIB structure and is examined in the Section 7.2. Here, we consider the random-access technique.

It is relatively easy to deduce the type of referencing convention that must be used. A table consists of a set of zero or more rows. Each row contains the same set of scalar object types, or columnar objects. Each columnar object has a unique object identifier that is the same in each row. For example, looking back at Figure 5.6, there are three instances of `tcpConnState`, but all three instances have the same object identifier: 1.3.6.1.2.1.6.13.1.1. Now, as was described in Chapter 5, the values of the `INDEX` objects of a table are used to distinguish one row from another. Thus, a combination of the object identifier for a columnar object and one set of values of the `INDEX` objects specifies a particular scalar object in a particular row of the table. The convention used in SNMP is to concatenate the scalar object identifier with the values of the `INDEX` objects, listed in the order in which the `INDEX` objects appear in the table definition.

As a simple example, consider the `ifTable` in the `interfaces` group. There is only one `INDEX` object, `ifIndex`, whose value is an integer in the range between 1 and the value of `ifNumber`, with each interface being assigned a unique number. Now suppose that we want to know the interface type of the second interface of a system. The object identifier of `ifType` is 1.3.6.1.2.1.2.2.1.3. The value of `ifIndex` of interest is 2. So the instance identifier for the instance of `ifType` corresponding to the row containing a value of `ifIndex` of 2 is 1.3.6.1.2.1.2.2.1.3.2. We have simply added the value of `ifIndex` as the final subidentifier in the instance identifier.

For a more complicated case, consider the `tcpConnTable` in the `tcp` group. As indicated in Figures 5.5 and 6.10, this table has four `INDEX` objects. Thus, an instance identifier for any of

Notes

1. The ASN.1 standard uses the term "basic ASN.1 type" to refer to any ASN.1 type that is not a macro instance.
2. This example is found in the ASN.1 standard.
3. For a more complete discussion of two's complement representation and two's complement arithmetic, see (Stallings 1996b).

Glossary

Some of the definitions in this glossary are from the *American National Standard Dictionary of Information Technology*, ANSI Standard X3.172, 1995. These entries are marked with an asterisk.

Abstract Syntax Notation One (ASN.1)
A formal language used to define syntax. In the case of SNMP, ASN.1 notation is used to define the format of SNMP protocol data units and of objects.

accounting management
One of the five OSI systems management functional areas (SMFAs). Consists of facilities that enable the detection, isolation, and correction of abnormal operation of the OSI environment.

agent
In the context of SNMP, a software module that performs the network management functions requested by network management stations. An agent module may be implemented in any network element that is to be managed, such as a host, bridge, or router. Agents and network management stations communicate by means of SNMP.

application layer
Layer 7 of the OSI model. This layer determines the interface of the system with the user and provides useful application-oriented services.

availability
The percentage of time that a particular function or application is available for users.

bridge*
A functional unit that interconnects two local-area networks (LANs) that use the same logical link control protocol but may use different medium access control protocols.

bus
A LAN topology in which stations are attached to a shared transmission medium. The medium is a linear cable; transmissions propagate the length of the medium and are received by all stations.

byte
A group of bits, usually eight, used to represent a character or other data.

columnar object
An object that is part of an SNMP table. There is one instance of the columnar object for each row in the table.

communications architecture
The hardware and software structure that implements the communications function.

community
In the context of SNMP, a relationship between an agent and a set of SNMP managers that defines security characteristics. The community

concept is a local one, defined at the agent. The agent establishes one community for each desired combination of authentication, access control, and proxy characteristics. Each community is given a unique (within this agent) community name, and the management stations within that community are provided with and must employ the community name in all get and set operations. The agent may establish a number of communities, with overlapping management station membership.

configuration management
One of the five OSI systems management functional areas (SMFAs). Consists of facilities that exercise control over, identify, collect data from, and provide data to managed objects for the purpose of assisting in providing for continuous operation of interconnection services.

counter
A nonnegative integer that may be incremented but not decremented. The maximum value is determined by the number of bits assigned to the counter. When the counter reaches its maximum, it wraps around and starts increasing again from zero. In SNMPv1, all counters are 32 bits; SNMPv2 also allows 64-bit counters.

cyclic redundancy check (CRC)
An error-detecting code in which the code is the remainder resulting from dividing the bits to be checked by a predetermined binary number.

datagram*
In packet switching, a packet, independent of other packets, that carries information sufficient for routing from the originating data terminal equipment (DTE) to the destination DTE without the necessity of establishing a connection between the DTEs and the network.

data link layer*
In OSI, the layer that provides service to transfer data between network-layer entities, usually in adjacent nodes. The data link layer detects and possibly corrects errors that may occur in the physical layer.

end system (ES)
A device other than an intermediate system attached to a subnetwork in an internet. End systems on different subnetworks exchange data by transmitting the data through one or more intermediate systems.

encapsulation
The addition of control information by a protocol entity to data obtained from a protocol user.

encrypt*
To convert plain text or data into unintelligible form by the use of a code in such a manner that reconversion to the original form is possible.

error-detecting code*
A code in which each coded representation conforms to specific rules of construction, so that their violation indicates the presence of errors.

error rate*
The number errors per unit of time.

fault management
One of the five OSI systems management functional areas (SMFAs). Consists of facilities that enable the detection, isolation, and correction of abnormal operation of the OSI environment.

flow control
A function performed by a receiving entity to limit the amount or rate of data sent by a transmitting entity.

frame
A group of bits that includes data plus one or more addresses and other protocol control information. Generally refers to a link layer (OSI layer 2) protocol data unit.

frame check sequence (FCS)
An error-detecting code inserted as a field in a block of data to be transmitted. The code serves to check for errors upon reception of the data.

gateway

An internetworking device that connects two computer networks that use different communications architectures.

gauge

A nonnegative integer that may increase or decrease with a range between 0 and some maximum value.

header

System-defined control information that precedes user data.

intermediate system (IS)

A device that is attached to two or more subnetworks in an internet and that performs routing and relaying of data between end systems. Examples of intermediate systems are bridges and routers.

internet

A collection of communication networks interconnected by bridges, routers, and/or gateways.

Internet Protocol*

A protocol designed for use in interconnected systems of packet networks. The Internet Protocol provides for transmitting blocks of data, called datagrams, from sources to destinations, where source and destination are hosts identified by fixed-length addresses. The Internet Protocol also provides for fragmentation and reassembly of long datagrams, if necessary, for transmission through small-packet networks.

internetworking

Communication among devices across multiple networks.

layer*

A group of services, functions, and protocols that is complete from a conceptual point of view, that is one out of a set of hierarchically arranged groups, and that extends across all systems that conform to the network architecture.

logical link control (LLC)*

In a local-area network, the protocol that governs the exchange of frames between data stations independently of how the transmission medium is shared.

management information base (MIB)

In the context of SNMP, this term is used in two ways: (1) A structured set of data variables, called objects, in which each variable represents some resource to be managed. Each agent in a network maintains a MIB for the network element on which it executes. (2) The definition of a related collection of objects that represent some related collection of resources to be managed. A number of MIBs, in the sense of definition (2), have been issued as RFCs.

medium access control (MAC)*

In a local-area network, the protocol that governs access to the transmission medium, taking into account the topological aspects of the network, to enable the exchange of data between data stations.

network layer

Layer 3 of the OSI model. Responsible for routing data through a communication network.

network management station

In the context of SNMP, a software module that executes management applications that monitor and control network elements, such as hosts, bridges, and routers. A network management station communicates with an agent in a network element by means of SNMP.

network-monitoring system

An integrated set of hardware and software that measures and analyzes communications-related parameters in a network.

network technical control system

A system, consisting of hardware probes and supporting software, that deals with fault detection, fault isolation, and fault recovery.

object

In the context of SNMP, a data variable that represents some resource or other aspect of a managed device; also referred to as a managed object. Note that this definition is quite different from the normal use of the term "object" in the context of object-oriented design.

object identifier

Uniquely identifies an object within a MIB. The form of an object identifier is a sequence of numbers separated by periods. This sequence defines the location of an object in the tree-structured MIB of which it is a part.

object instance

A specific instance of an object type that has been bound to a specific value.

object type

Defines a particular kind of managed object. The definition of an object type is therefore a syntactic description.

octet

A group of eight bits, usually operated upon as an entity.

Open Systems Interconnection (OSI) reference model

A model of communications between cooperating devices. It defines a seven-layer architecture of communication functions.

packet

A group of bits that includes data plus control information. Generally refers to a network-layer (OSI layer 3) protocol data unit.

packet switching

A method of transmitting messages through a communications network, in which long messages are subdivided into short packets. Each packet is passed from source to destination through intermediate nodes. At each node, the entire message is received, stored briefly, and then passed on to the next node.

performance management

One of the five OSI systems management functional areas (SMFAs). Consists of facilities needed to evaluate the behavior of managed objects and the effectiveness of communication activities.

physical layer

Layer 1 of the OSI model. Concerned with the electrical, mechanical, and timing aspects of signal transmission over a medium.

presentation layer*

Layer 6 of the OSI model. Provides for the selection of a common syntax for representing data and for transformation of application data into and from the common syntax.

probe

In the context of RMON, a remote network monitor.

propagation delay

The delay between the time a signal enters a channel and the time it is received.

protocol*

A set of semantic and syntactic rules that determines the behavior of entities in the same layer in performing communication functions.

protocol control information*

Information exchanged between entities of a given layer, via the service provided by the next lower layer, to coordinate their joint operation.

protocol data unit (PDU)*

A set of data specified in a protocol of a given layer and consisting of protocol control information of that layer, and possibly user data of that layer.

proxy

In the context of SNMP, an agent (the proxy agent) that acts on behalf of another network element (the proxied device). A management station sends queries concerning a device to its proxy agent. The proxy agent is responsible for collecting the information or triggering the action requested of the proxied device by the management station.

remote network monitor

An agent, implemented in a network element, that observes all of the traffic on the network or networks and maintains information and statistics concerning that traffic in its MIB. Also referred to as a probe.

response time

In a data system, the elapsed time between the end of transmission of an inquiry message and the beginning of the receipt of a response message, measured at the inquiry terminal.

router

An internetworking device that connects two computer networks. It makes use of an internet protocol and assumes that all of the attached devices on the networks use the same communications architecture and protocols. A router operates at OSI layer 3.

routing

The determination of a path that a data unit (frame, packet, message) will traverse from source to destination.

security management

One of the five OSI systems management functional areas (SMFAs). Addresses those aspects of OSI security essential to operate OSI network management correctly and to protect managed objects.

service access point (SAP)

A means of identifying a user of the services of a protocol entity. A protocol entity provides one or more SAPs, for use by higher-level entities.

session layer

Layer 5 of the OSI model. Manages a logical connection (session) between two communicating processes or applications.

software monitor

A software module resident in main memory on a host or communications processor that can gather and report statistics on configuration and communications and software activity.

subnetwork

Refers to a constituent network of an internet. This avoids ambiguity since the entire internet, from a user's point of view, is a single network.

systems management function (SMF)

A part of OSI systems management activities that satisfies a set of logically related user requirements.

systems management functional area (SMFA)

A category of OSI systems management user requirements.

transport layer

Layer 4 of the OSI model. Provides reliable, sequenced transfer of data between endpoints.

trap

In the context of SNMP, an unsolicited message sent by an agent to a management station. The purpose is to notify the management station of some unusual event.

virtual circuit

A packet-switching mechanism in which a logical connection (virtual circuit) is established between two stations at the start of transmission. All packets follow the same route, need not carry a complete address, and arrive in sequence.

References

Ben-Artzi, A.; Chandna, A.; and Warrier, U. (1990). "Network Management of TCP/IP Networks: Present and Future." *IEEE Network Magazine,* July.

Boardman, B., and Morrissey, P. (1995). "Probing the Depths of RMON." *Network Computing,* February 1.

Case, J., and Partridge, C. (1989). "Case Diagrams: A First Step to Diagrammed Management Information Bases." *Computer Communication Review,* January. Reprinted in *Connexions,* March.

Cerf, V. (1988). *IAB Recommendations for the Development of Internet Management Standards.* RFC 1052, April.

Cerf, V. (1989). *Report of the Second Ad Hoc Network Management Review Group.* RFC 1109, August.

Chiu, D., and Sudama, R. (1992). *Network Monitoring Explained: Design and Application.* New York: Ellis Horwood.

Dupuy, A., et al. (1989). "Network Fault Management: A User's View." *Proceedings, First International Symposium on Integrated Network Management,* May; published by North-Holland.

Eckerson, W. (1992). "Net Management Traffic Can Sap Net Performance." *Network World,* May 14.

Fried, S., and Tjong, J. (1990). "Implementing Integrated Monitoring Systems for Heterogeneous Networks." In (Kerchenbaum 1990).

Guynes, J. (1988). "Impact of System Response Time on State Anxiety." *Communications of the ACM,* March.

Jacobson, V. (1988). "Congestion Avoidance and Control." *Proceedings, SIGCOMM '88,* August.

Kerchenbaum, A.; Malek, M.; and Wall, M. eds. (1990). *Network Management and Control.* New York: Plenum.

Martin, J. (1988). *Principles of Data Communication.* Englewood Cliffs, NJ: Prentice-Hall.

Mazumdar, S., and Lazar, A. (1991). "Objective-Driven Monitoring." *Proceedings, Second*

International Symposium on Integrated Network Management, April; published by North-Holland.

Mier, E. (1991a). "Network World, Bell Labs Evaluate SNMP on Bridges." *Network World,* April 22.

Mier, E. (1991b). "Network World, Bell Labs Test Routers' SNMP Agents." *Network World,* July 1.

Shneiderman, B. (1984). "Response Time and Display Rate in Human Performance with Computers." *ACM Computing Surveys*, September.

Smith, D. (1983). "Faster Is Better: A Business Case for Subsecond Response Time." *Computerworld*, April 18.

Stallings, W. (1993). *Networking Standards: A Guide to OSI, ISDN, LAN, and MAN Standards.* Reading, MA: Addison-Wesley.

Stallings, W. (1995a). *Network and Internetwork Security: Principles and Practice.* Englewood Cliffs, NJ: Prentice-Hall.

Stallings, W. (1995b). *Operating Systems.* Englewood Cliffs, NJ: Prentice-Hall.

Stallings, W. (1996a). *Local and Metropolitan Area Networks,* 5th ed. Englewood Cliffs, NJ: Prentice-Hall.

Stallings, W. (1996b). *Computer Organization and Architecture,* 4th ed. Englewood Cliffs, NJ: Prentice-Hall.

Stallings, W. (1996c). *Data and Computer Communications,* 5th ed. Englewood Cliffs, NJ: Prentice-Hall.

Terplan, K. (1992). *Communication Networks Management.* Englewood Cliffs, NJ: Prentice-Hall.

Thadhani, A. (1981). "Interactive User Productivity." *IBM Systems Journal*, no. 1.

Thomas, R. (1995). "Interoperable RMON? Plug and Pray." *Data Communications*, May.

Waldbusser, S. (1992). "Applications Stand to Benefit from SNMP." *The Simple Times,* September/October 1992.

Wilkinson, S., and Capen, T. (1992). "Remote Control." *Corporate Computing,* October.

Index

List of Acronyms

ACSE	Association Control Service Element
ANSI	American National Standards Institute
ASN.1	Abstract Syntax Notation One
FTP	File Transfer Protocol
IAB	Internet Architecture Board
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standardization
LAN	local-area network
MIB	management information base
OSI	Open Systems Interconnection
PDU	protocol data unit
RFC	Request for Comment
RMON	Remote Network Monitoring
SMI	structure of management information
SMP	Simple Management Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol

List of Acronyms

ACSE	Association Control Service Element
ANSI	American National Standards Institute
ASN.1	Abstract Syntax Notation One
FTP	File Transfer Protocol
IAB	Internet Architecture Board
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standardization
LAN	local-area network
MIB	management information base
OSI	Open Systems Interconnection
PDU	protocol data unit
RFC	Request for Comment
RMON	Remote Network Monitoring
SMI	structure of management information
SMP	Simple Management Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol