Includes latest SNMPv2 and RMON2 specs

SNMP SNMPv2 *and* RMON

Practical Network Management
Second Edition

William Stallings

SNMP, SNMPv2, and RMON

Practical Network Management

Second Edition

William Stallings

ADDISON-WESLEY
An imprint of Addison Wesley Longman, Inc.
Reading, Massachusetts Harlow, England Menlo Park, California
Berkeley, California Don Mills, Ontario Sydney
Bonn Amsterdam Tokyo Mexico City

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

Text printed on recycled and acid-free paper

4 5 6 7 8 9 MA 00 99 98 97

4th Printing November, 1997

SNMP, SNMPv2, and RMON

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

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).

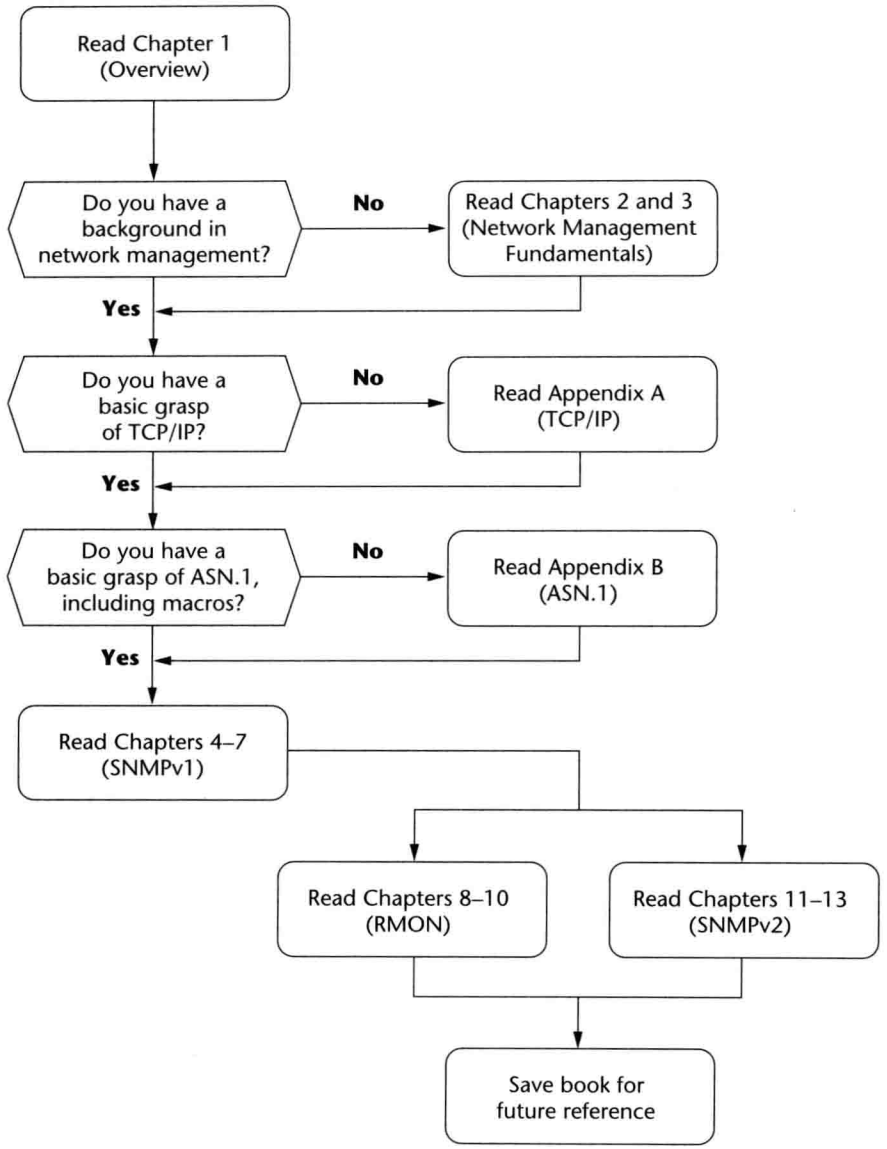


FIGURE P.1 **A Reading Guide**

Contents

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:

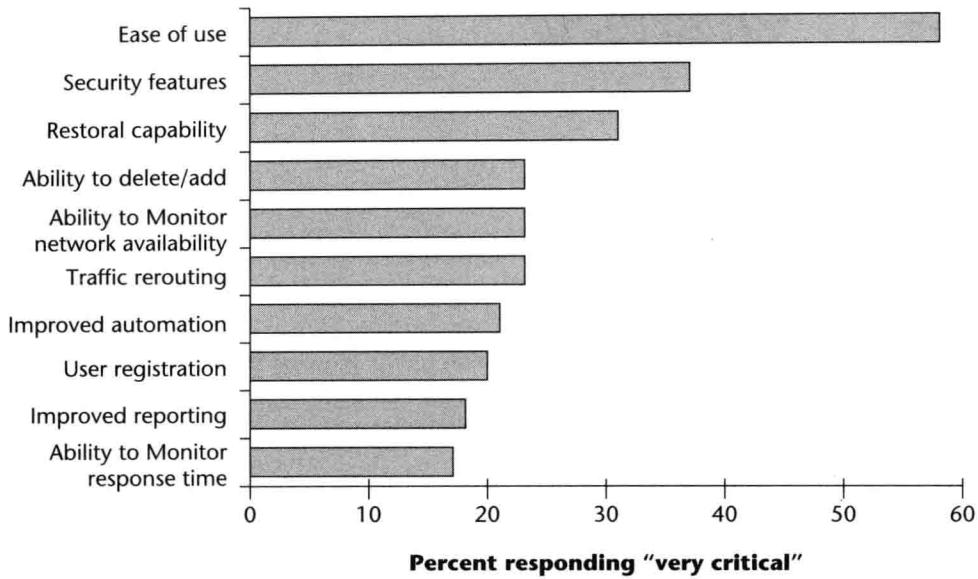
- The network and its associated resources and distributed applications become indispensable to the organization.
- More things can go wrong, disabling the network or a portion of the network, or degrading performance to an unacceptable level.

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