Help for System and Network Administrators

2nd Edition

Essential SNMP

O'REILLY®

Douglas R. Mauro & Kevin J. Schmidt

O'REILLY®

Essential SNMP

Essential SNMP, Second Edition, is a practical guide for system and network administrators using the Simple Network Management Protocol to manage their servers and routers. It starts with the basics of SNMP and how it works, covering technical elements such as OIDs, MIBs, community strings, and traps. More importantly, this book shows you how to use SNMP to keep track of what your network is doing. *Essential SNMP* focuses on practical system and network administration, how to configure SNMP agents and network management stations, how to use SNMP to retrieve and modify variables on network devices, and how to configure management software to react to traps sent by managed devices.

Now in its second edition, *Essential SNMP* has been thoroughly revised and expanded, and includes numerous Perl scripts to help you automate more of your management tasks. You'll find scripts for service monitoring techniques for SMTP, POP3, HTTP, and DNS, a Perl-based SNMP agent, switch port control, usage of the Cisco Ping MIB, a section on wireless access point (WAP) monitoring, and a brand-new chapter on Java and SNMP.

Essential SNMP is filled with practical examples of a variety of tools, from popular commercial products such as HP's OpenView and Castle Rock's SNMPc to a rich variety of open source tools. You'll find a new chapter on RRDtool and Cricket, a new appendix on open source network management systems, and expanded coverage of SNMPv3. *Essential SNMP* is the book you need to get a handle on your network and manage it effectively.

"Essential SNMP *gives you the system administrator's perspective on SNMP: what it is, and, more importantly, practical examples of how to integrate SNMP into the administrator's toolset. If you need to know about user activity, errant core files, and misbehaving printers, SNMP will do all the heavy lifting for you.* Essential SNMP *gives you the power to harness SNMP without breaking into a sweat.*"

—Dr. Marshall T. Rose, former Network Management Area Director of the IETF

"Finally, a practical book on SNMP and network management that does not simply regurgitate the standards. Essential SNMP *is a must-read for any network and system administrator or anyone who actually has to use SNMP to monitor and troubleshoot networks, systems, and applications. A copy of this book should be kept right alongside any NMS."*

—Robert Krupczak, PhD, Founder, Empire Technologies, and Chief Scientist, the Krupczak Organization

"This is definitely the book I would most recommend to anyone using SNMP for network management. It truly covers the essentials—from concepts through tools, applications, examples, and extensibility to fit particular needs."

—Dr. Robert Minch, Professor, Boise State University

www.oreilly.com

US $49.95 **CAN $69.95**

ISBN: 978-0-596-00840-6

9 780596 008406 54995

easy computing

Essential SNMP

Other resources from O'Reilly

Related titles

- IPv6 Network Administration
- Ethernet: The Definitive Guide
- 802.11 Wireless Networks: The Definitive Guide
- DNS and BIND

oreilly.com

oreilly.com is more than a complete catalog of O'Reilly books. You'll also find links to news, events, articles, weblogs, sample chapters, and code examples.

oreillynet.com is the essential portal for developers interested in open and emerging technologies, including new platforms, programming languages, and operating systems.

Conferences

O'Reilly brings diverse innovators together to nurture the ideas that spark revolutionary industries. We specialize in documenting the latest tools and systems, translating the innovator's knowledge into useful skills for those in the trenches. Visit *conferences.oreilly.com* for our upcoming events.

Safari Bookshelf (*safari.oreilly.com*) is the premier online reference library for programmers and IT professionals. Conduct searches across more than 1,000 books. Subscribers can zero in on answers to time-critical questions in a matter of seconds. Read the books on your Bookshelf from cover to cover or simply flip to the page you need. Try it today with a free trial.

SECOND EDITION

Essential SNMP

Douglas R. Mauro and Kevin J. Schmidt

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Paris • Sebastopol • Taipei • Tokyo

Essential SNMP, Second Edition
by Douglas R. Mauro and Kevin J. Schmidt

Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

Editors: Michael Loukides and Debra Cameron

Production Editor: Darren Kelly

Cover Designer: Ellie Volckhausen

Interior Designer: David Futato

Printing History:

July 2001: First Edition.

September 2005: Second Edition.

This book uses RepKover™, a durable and flexible lay-flat binding.

ISBN: 0-596-00840-6
ISBN13: 978-0-596-00840-6
[M]

easy computing

[02/08]

Table of Contents

Preface

The Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. Many kinds of devices support SNMP, including routers, switches, servers, workstations, printers, modem racks, and uninterruptible power supplies (UPSs). The ways you can use SNMP range from the mundane to the exotic: it's fairly simple to use SNMP to monitor the health of your routers, servers, and other pieces of network hardware, but you can also use it to control your network devices, page someone, or take other automatic actions if problems arise. The information you can monitor ranges from relatively simple and standardized items, like the amount of traffic flowing into or out of an interface, to more esoteric hardware- and vendor-specific items, like the air temperature inside a router.

Given that there are already a number of books about SNMP in print, why write another one? Although there are many books on SNMP, there's a lack of books aimed at the practicing network or system administrator. Many books cover how to implement SNMP or discuss the protocol at a fairly abstract level, but none really answers the network administrator's most basic questions: how can I best put SNMP to work on my network? How can I make managing my network easier?

We provide a brief overview of the SNMP protocol in Chapters 2 and 3 and then spend a few chapters discussing issues such as hardware requirements and the sorts of tools that are available for use with SNMP. However, the bulk of this book is devoted to discussing, with real examples, how to use SNMP for system and network administration tasks.

Most newcomers to SNMP ask some or all of the following questions:

- What exactly is SNMP?
- How can I, as a system or network administrator, benefit from SNMP?
- What is a MIB?
- What is an OID?
- What is a community string?

- What is a trap?
- I've heard that SNMP is insecure. Is this true?
- Do any of my devices support SNMP? If so, how can I tell if they are configured properly?
- How do I go about gathering SNMP information from a device?
- I have a limited budget for purchasing network management software. What sort of free/open source software is available?
- Is there an SNMP Perl module that I can use to write cool scripts?
- Can I use Java™ to work with SNMP?

This book answers all these questions and more. Our goal is to demystify SNMP and make it more accessible to a wider range of users.

Audience for This Book

This book is intended for system and network administrators who could benefit from using SNMP to manage their equipment but who have little or no experience with SNMP or SNMP applications. In our experience, almost any network, no matter how small, can benefit from using SNMP. If you're a Perl programmer, this book will give you some ideas about how to write scripts that use SNMP to help manage your network. If you're not a Perl user, you can use many of the other tools we present, ranging from Net-SNMP (an open source collection of command-line tools) to Hewlett-Packard's OpenView (a high-end, high-priced network management platform).

Organization

Chapter 1, *Introduction to SNMP and Network Management*, provides a nontechnical overview of network management with SNMP. We introduce the different versions of SNMP, managers and agents, network management concepts, and change management techniques.

Chapter 2, *SNMPv1 and SNMPv2*, discusses the technical details of SNMP versions 1 and 2. We look at the Structure of Management Information (SMI) and the Management Information Base (MIB) and discuss how SNMP actually works—how management information is sent and received over the network.

Chapter 3, *SNMPv3*, discusses SNMP version 3, which is now a full standard that provides robust security for SNMP.

Chapter 4, *NMS Architectures*, helps you to think through strategies for deploying SNMP.

Chapter 5, *Configuring Your NMS*, provides a basic understanding of what to expect when installing NMS software by looking at two NMS packages, HP's OpenView and Castle Rock's SNMPc.

Chapter 6, *Configuring SNMP Agents*, describes how to configure several SNMP agents for Unix and Windows, including the Net-SNMP agent. To round out the chapter, we discuss how to configure the embedded agents on two network devices: the Cisco SNMP agent and the APC Symetra SNMP agent.

Chapter 7, *Polling and Setting*, shows how you can use command-line tools and Perl to gather (poll) SNMP information and change (set) the state of a managed device.

Chapter 8, *Polling and Thresholds*, discusses how to configure OpenView and SNMPc to gather SNMP information via polling. This chapter also discusses RMON configuration on a Cisco router.

Chapter 9, *Traps*, examines how to send and receive traps using command-line tools, Perl, OpenView, and other management applications.

Chapter 10, *Extensible SNMP Agents*, shows how several popular SNMP agents can be extended. Extensible agents provide end users with a means to extend the operation of an agent without having access to the agent's source code.

Chapter 11, *Adapting SNMP to Fit Your Environment*, is geared toward Perl-savvy system administrators. We provide Perl scripts that demonstrate how to perform some common system administration tasks with SNMP.

Chapter 12, *MRTG*, introduces one of the most widely used open source SNMP applications, the Multi Router Traffic Grapher (MRTG). MRTG provides network administrators with web-based usage graphs of router interfaces and can be configured to graph many other kinds of data.

Chapter 13, *RRDtool and Cricket*, introduces RRDtool and Cricket. Used together, these tools provide graphing techniques like those in MRTG, but with added flexibility.

Chapter 14, *Java and SNMP*, discusses how to use Java to build SNMP applications.

Appendix A, *Using Input and Output Octets*, discusses how to use OpenView to graph input and output octets.

Appendix B, *More on OpenView's NNM*, discusses how to graph external data with Network Node Manager (NNM), add menu items to NNM, configure user profiles, and use NNM as a centralized communication interface.

Appendix C, *Net-SNMP Tools*, summarizes the usage of the Net-SNMP command-line tools.

Appendix D, *SNMP RFCs*, provides an authoritative list of the various RFC numbers that pertain to SNMP.

Appendix E, *SNMP Support for Perl*, is a good summary of the SNMP Perl module used throughout the book along with an introduction to the Net-SNMP Perl module.

Appendix F, *Network Management Software*, presents an overview of network management software by category.

Appendix G, *Open Source Monitoring Software*, introduces some commonly used open source network management and monitoring tools.

Appendix H, *Network Troubleshooting Primer*, provides a primer on tools that can aid in network troubleshooting.

What's New in This Edition

This second edition has been thoroughly revised and expanded. It includes the following new features:

- Chapter 1 includes coverage of the concepts behind network management and change management.
- Chapter 2 provides packet traces of the various SNMP operations.
- Chapter 3 provides coverage of SNMPv3. This chapter was an appendix in the first edition; it has been expanded to a full chapter.
- SNMPc coverage has been expanded in Chapters 5 and 9.
- Chapter 11 explains the use of scripts for a variety of tasks. This chapter has doubled in size to include many new scripts. You'll find scripts for service monitoring techniques for SMTP, POP3, HTTP, and DNS, a Perl-based SNMP agent, switch port control, usage of the Cisco Ping MIB, and a section on wireless access point (WAP) monitoring.
- Chapter 13, new in this edition, discusses RRDtool and Cricket.
- Chapter 14, also new in this edition, is devoted to showing how Java can be used to create SNMP applications.
- Appendix E provides a brief overview of Net-SNMP's Perl module.
- Appendix G provides details on the most commonly used open source tools for network management and monitoring.
- Appendix H introduces the most commonly used network troubleshooting tools.

Example Programs

All the example programs in this book are available from this book's web page at *http://www.oreilly.com/catalog/esnmp2/*

Using Code Examples

This book is here to help you get your job done. In general, you may use the code in this book in your programs and documentation. You do not need to contact O'Reilly for permission unless you're reproducing a significant portion of the code. For example, writing a program that uses several chunks of code from this book does not require permission. Selling or distributing a CD-ROM of examples from O'Reilly books *does* require permission. Answering a question by citing this book and quoting example code does not require permission. Incorporating a significant amount of example code from this book into your product's documentation *does* require permission.

We appreciate, but do not require, attribution. An attribution usually includes the title, author, publisher, and ISBN. For example: "*Essential SNMP*, Second Edition, by Douglas R. Mauro and Kevin J. Schmidt. Copyright 2005 O'Reilly Media, Inc., 0-596-00840-6."

If you feel your use of code examples falls outside fair use or the permission given above, feel free to contact us at *permissions@oreilly.com*.

Conventions Used in This Book

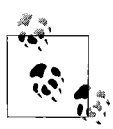
The following typographical conventions are used in this book:

Italic
: Used for object IDs, URLs, filenames, and directory names. It is also used for emphasis and for the first use of technical terms.

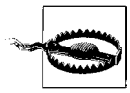
`Constant width`
: Used for examples, object definitions, literal values, textual conventions, and datatypes. It is also used to show source code, the contents of files, and the output of commands.

`Constant width bold`
: Used in interactive examples to show commands or text that would be typed literally by the user. It is also used to emphasize when something, usually in source code or file-contents examples, has been added to or changed from a previous example.

`Constant width italic`
: Used for replaceable parameter names in command syntax.



Indicates a tip, suggestion, or general note.



Indicates a warning or caution.

Comments and Questions

Please address comments and questions concerning this book to the publisher:

O'Reilly Media, Inc.
1005 Gravenstein Highway North
Sebastopol, CA 95472
(800) 998-9938 (in the United States or Canada)
(707) 829-0515 (international/local)
(707) 829-0104 (fax)

There is a web page for this book, which lists errata, code examples, reviews, and any additional information. You can access this page at:

http://www.oreilly.com/catalog/esnmp2/

To comment or ask technical questions about this book, send email to:

bookquestions@oreilly.com

For more information about books, conferences, software, Resource Centers, and the O'Reilly Network, see the O'Reilly web site at:

http://www.oreilly.com

Safari® Enabled

When you see a Safari® Enabled icon on the cover of your favorite technology book, it means the book is available online through the O'Reilly Network Safari Bookshelf.

Safari offers a solution that's better than e-books. It's a virtual library that lets you easily search thousands of top technology books, cut and paste code samples, download chapters, and find quick answers when you need the most accurate, current information. Try it for free at *http://safari.oreilly.com*.

Acknowledgments for the Second Edition

Deb Cameron deserves a big thank you for shepherding this second edition from beginning to end. Her diligence and effort helped keep us on track. Dr. Robert Minch, professor at Boise State University, provided valuable suggestions for the second edition. Bobby Krupczak, Ph.D., [illegible] provided feedback on the Concord SystemEDGE agent. Frank Fock was kind enough to provide comments on the Java

and SNMP chapter. Max Baker provided the idea for the channel-setting algorithm presented in Chapter 11. Jim Boney graciously volunteered the use of his Cisco routers. Castle Rock Computing was gracious enough to provide us with a copy of SNMPc for the second edition of this book; special thanks go to Castle Rock's John Maytum for coordinating our access to SNMPc.

We are grateful for input from Jason Briggs, Bill Horsfall, and Jason Weiss, who reviewed new material for this second edition under a very tight schedule.

Douglas

For years I worked as a system and network administrator and often faced the question, "How are things running?" This is what led me to SNMP and eventually to the idea for this book. Of course, I would like to thank Kevin for his hard work and dedication. Special thanks go to three special people in my life: my wife, Amy, and our children, Kari and Matthew, for putting up with my long absences while I was writing in the computer room. Thanks also go to my family and friends, who provided support and encouragement.

Kevin

Working on the second edition has been a great joy. The first edition has been out for almost four years, and in this time I have thought about what I wanted to add if someday O'Reilly wanted a second edition written. So, a thank you goes to O'Reilly for giving me the chance to update this book. I would like to thank Douglas for allowing me to once again work on the book with him. Finally, I would like to thank Danette, my loving and generous wife, for allowing me the time I needed to complete this project. Without her support, I would not have made it through the process.

Acknowledgments for the First Edition

It would be an understatement to say that this book was a long time in the making. It would never have been published without the patience and support of Michael Loukides. Thanks Mike! We would also like to thank the individuals who provided us with valuable technical review feedback and general help and guidance: Mike DeGraw-Bertsch at O'Reilly; Donald Cooley at Global Crossing; Jacob Kirsch at Sun Microsystems, Inc.; Bobby Krupczak, Ph.D., at Concord Communications; John Reinhardt at Road Runner; Patrick Bailey and Rob Sweet at Netrail; and Jürgen Schönwälder at the Technical University of Braunschweig. Rob Romano, a talented graphic artist at O'Reilly, deserves a thank you for making the figures throughout the book look great. Finally, thanks to Jim Sumser, who took the project over in its final stages, and to Rachel Wheeler, the production editor, for putting this book together.


easy
computing

CHAPTER 1

Introduction to SNMP and Network Management

In today's complex network of routers, switches, and servers, it can seem like a daunting task to manage all the devices on your network and make sure they're not only up and running but also performing optimally. This is where the Simple Network Management Protocol (SNMP) can help. SNMP was introduced in 1988 to meet the growing need for a standard for managing Internet Protocol (IP) devices. SNMP provides its users with a "simple" set of operations that allows these devices to be managed remotely.

This book is aimed toward system administrators who would like to begin using SNMP to manage their servers or routers, but who lack the knowledge or understanding to do so. We try to give you a basic understanding of what SNMP is and how it works; beyond that, we show you how to put SNMP into practice, using a number of widely available tools. Above all, we want this to be a practical book—a book that helps you keep track of what your network is doing.

This chapter introduces SNMP, network management, and change management. Obviously, SNMP is the focus of this book, but having an understanding of general network management concepts will make you better prepared to use SNMP to manage your network.

What Is SNMP?

The core of SNMP is a simple set of operations (and the information these operations gather) that gives administrators the ability to change the state of some SNMP-based device. For example, you can use SNMP to shut down an interface on your router or check the speed at which your Ethernet interface is operating. SNMP can even monitor the temperature on your switch and warn you when it is too high.

SNMP usually is associated with managing routers, but it's important to understand that it can be used to manage many types of devices. While SNMP's predecessor, the Simple Gateway Management Protocol (SGMP), was developed to manage Internet routers, SNMP can be used to manage Unix systems, Windows systems, printers,

modem racks, power supplies, and more. Any device running software that allows the retrieval of SNMP information can be managed. This includes not only physical devices but also software, such as web servers and databases.

Another aspect of network management is network monitoring; that is, monitoring an entire network as opposed to individual routers, hosts, and other devices. Remote Network Monitoring (RMON) was developed to help us understand how the network itself is functioning, as well as how individual devices on the network are affecting the network as a whole. It can be used to monitor not only LAN traffic, but WAN interfaces as well. We discuss RMON in more detail later in this chapter and in Chapter 2.

RFCs and SNMP Versions

The Internet Engineering Task Force (IETF) is responsible for defining the standard protocols that govern Internet traffic, including SNMP. The IETF publishes Requests for Comments (RFCs), which are specifications for many protocols that exist in the IP realm. Documents enter the standards track first as *proposed* standards, then move to *draft* status. When a final draft is eventually approved, the RFC is given *standard* status—although there are fewer completely approved standards than you might think. Two other standards-track designations, *historical* and *experimental*, define (respectively) a document that has been replaced by a newer RFC and a document that is not yet ready to become a standard. The following list includes all the current SNMP versions and the IETF status of each (see Appendix D for a full list of the SNMP RFCs):

- SNMP Version 1 (SNMPv1) is the initial version of the SNMP protocol. It's defined in RFC 1157 and is a historical IETF standard. SNMPv1's security is based on communities, which are nothing more than passwords: plain-text strings that allow any SNMP-based application that knows the strings to gain access to a device's management information. There are typically three communities in SNMPv1: *read-only*, *read-write*, and *trap*. It should be noted that while SNMPv1 is historical, it is still the primary SNMP implementation that many vendors support.
- SNMP version 2 (SNMPv2) is often referred to as community-string-based SNMPv2. This version of SNMP is technically called SNMPv2c, but we will refer to it throughout this book simply as SNMPv2. It's defined in RFC 3416, RFC 3417, and RFC 3418.
- SNMP version 3 (SNMPv3) is the latest version of SNMP. Its main contribution to network management is security. It adds support for strong authentication and private communication between managed entities. In 2002, it finally made the transition from draft standard to full standard. The following RFCs define the standard: RFC [illegible] RFC 3[illegible]412, RFC 3413, RFC 3414, RFC 3415, RFC 3416, RFC 3417, RFC 3418, and RFC 2576. Chapter 3 provides a thorough treatment of SNMPv3 and Chapter 6 goes through the SNMPv3 agent

configuration for Net-SNMP and Cisco. While it is good news that SNMPv3 is a full standard, vendors are notoriously slow at adopting new versions of a protocol. While SNMPv1 has been transitioned to historical, the vast majority of vendor implementations of SNMP are SNMPv1 implementations. Some large infrastructure vendors like Cisco have supported SNMPv3 for quite some time, and we will undoubtedly begin to see more vendors move to SNMPv3 as customers insist on more secure means of managing networks.

The official site for RFCs is *http://www.ietf.org/rfc.html*. One of the biggest problems with RFCs, however, is finding the one you want. It is a little easier to navigate the RFC index at Ohio State University (*http://www.cse.ohio-state.edu/cs/Services/rfc/index.html*).

Managers and Agents

In the previous sections, we've vaguely referred to SNMP-capable devices and network management stations. Now it's time to describe what these two things really are. In the world of SNMP, there are two kind of entities: managers and agents. A *manager* is a server running some kind of software system that can handle management tasks for a network. Managers are often referred to as Network Management Stations (NMSs).* An NMS is responsible for polling and receiving traps from agents in the network. A *poll*, in the context of network management, is the act of querying an agent (router, switch, Unix server, etc.) for some piece of information. This information can be used later to determine if some sort of catastrophic event has occurred. A *trap* is a way for the agent to tell the NMS that something has happened. Traps are sent asynchronously, not in response to queries from the NMS. The NMS is further responsible for performing an action† based upon the information it receives from the agent. For example, when your T1 circuit to the Internet goes down, your router can send a trap to your NMS. In turn, the NMS can take some action, perhaps paging you to let you know that something has happened.

The second entity, the *agent*, is a piece of software that runs on the network devices you are managing. It can be a separate program (a daemon, in Unix language), or it can be incorporated into the operating system (for example, Cisco's IOS on a router, or the low-level operating system that controls a UPS). Today, most IP devices come with some kind of SNMP agent built in. The fact that vendors are willing to implement agents in many of their products makes the system administrator's or network manager's job easier. The agent provides management information to the NMS by keeping track of various operational aspects of the device. For example, the agent on a router is able to keep track of the state of each of its interfaces: which ones are up,

* See Appendix F for a listing of some popular NMS packages.
† Note that the NMS is preconfigured to perform the action.

which ones are down, etc. The NMS can query the status of each interface and take appropriate action if any of them are down. When the agent notices that something bad has happened, it can send a trap to the NMS. This trap originates from the agent and is sent to the NMS, where it is handled appropriately. Some devices will send a corresponding "all clear" trap when there is a transition from a bad state to a good state. This can be useful in determining when a problem situation has been resolved. Figure 1-1 shows the relationship between the NMS and an agent.

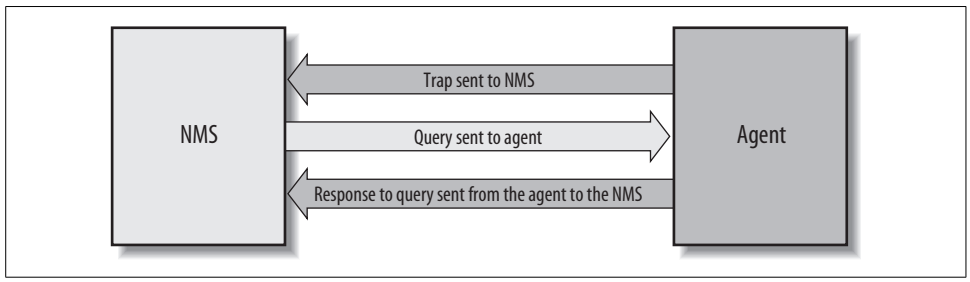


Figure 1-1. Relationship between an NMS and an agent

It's important to keep in mind that polls and traps can happen at the same time. There are no restrictions on when the NMS can query the agent or when the agent can send a trap.

The Structure of Management Information and MIBs

The Structure of Management Information (SMI) provides a way to define managed objects and their behavior. An agent has in its possession a list of the objects that it tracks. One such object is the operational status of a router interface (for example, *up*, *down*, or *testing*). This list collectively defines the information the NMS can use to determine the overall health of the device on which the agent resides.

The Management Information Base (MIB) can be thought of as a database of managed objects that the agent tracks. Any sort of status or statistical information that can be accessed by the NMS is defined in a MIB. The SMI provides a way to define managed objects while the MIB is the definition (using the SMI syntax) of the objects themselves. Like a dictionary, which shows how to spell a word and then gives its meaning or definition, a MIB defines a textual name for a managed object and explains its meaning. Chapter 2 goes into more technical detail about MIBs and the SMI.

An agent may implement many MIBs, but all agents implement a particular MIB called MIB-II* (RFC 1213). This standard defines variables for things such as inter-

* MIB-I is the original version of this MIB, but it is no longer referred to since MIB-II enhances it.

face statistics (interface speeds, MTU, octets* sent, octets received, etc.) as well as various other things pertaining to the system itself (system location, system contact, etc.). The main goal of MIB-II is to provide general TCP/IP management information. It doesn't cover every possible item a vendor may want to manage within its particular device.

What other kinds of information might be useful to collect? First, many draft and proposed standards have been developed to help manage things such as frame relay, ATM, FDDI, and services (mail, Domain Name System (DNS), etc.). A sampling of these MIBs and their RFC numbers includes:

- ATM MIB (RFC 2515)
- Frame Relay DTE Interface Type MIB (RFC 2115)
- BGP Version 4 MIB (RFC 1657)
- RDBMS MIB (RFC 1697)
- RADIUS Authentication Server MIB (RFC 2619)
- Mail Monitoring MIB (RFC 2789)
- DNS Server MIB (RFC 1611)

But that's far from the entire story, which is why vendors, and individuals, are allowed to define MIB variables for their own use.† For example, consider a vendor that is bringing a new router to market. The agent built into the router will respond to NMS requests (or send traps to the NMS) for the variables defined by the MIB-II standard; it probably also implements MIBs for the interface types it provides (e.g., RFC 2515 for ATM and RFC 2115 for Frame Relay). In addition, the router may have some significant new features that are worth monitoring but are not covered by any standard MIB. So, the vendor defines its own MIB (sometimes referred to as a *proprietary MIB*) that implements managed objects for the status and statistical information of its new router.

Simply loading a new MIB into your NMS does not necessarily allow you to retrieve the data/values/objects, etc., defined within that MIB. You need to load only those MIBs supported by the agents from which you're requesting queries (e.g., snmpget, snmpwalk). Feel free to load additional MIBs for future device support, but don't panic when your device doesn't answer (and possibly returns errors for) these unsupported MIBs.

* An octet is an 8-bit quantity which is the fundamental unit of data transfer in TCP/IP networks.

† This topic is discussed further in the next chapter.

About the Authors

Douglas R. Mauro received his bachelor's degree from the University of Albany, New York, and worked as a system administrator for several years before becoming a project engineer with Sun Microsystems, Inc. In addition to his consulting duties with Sun, he authors their internal OneStop Sun Management Center page and has published several InfoDocs with them.

Kevin J. Schmidt currently lives in Lilburn, Georgia. He is a senior software developer at Reflex Security, Inc. (*http://www.reflexsecurity.com*), where he gets to develop software in both Java and C. Prior to Reflex, Kevin spent four years at GuardedNet, Inc. (*http://www.guarded.net*) as a senior software developer and team lead.

Originally from Pensacola, Florida, Kevin moved to Atlanta in late 1996 to work for MindSpring Enterprises (now known as Earthlink, Inc.), a national ISP. He spent four years in network management and was the senior network management architect for Earthlink. He left Earthlink to work at Netrail, a tier-1 Internet backbone provider. While at Netrail, Kevin was in charge of the company's network management architecture.

Kevin's first computer was a Commodore 64. He began running Bulletin Board Systems (BBSs) at age 11 and later became interested in computer networking in general. His other computing interests include Linux, MySQL, programming languages, and theoretical computer science.

Colophon

Our look is the result of reader comments, our own experimentation, and feedback from distribution channels. Distinctive covers complement our distinctive approach to technical topics, breathing personality and life into potentially dry subjects.

The animals on the cover of *Essential SNMP*, Second Edition are red deer (*Cervus elaphus*). Male red deer, also known as *stags* or *harts*, can grow to over 400 pounds. and stand 42–54 inches tall at the shoulder. Females, or *hinds*, are more slightly built and usually reach a weight of only about 200 pounds. The color of the red deer's coat ranges from a warm reddish-brown in the summer to a darker grayish-brown in winter. Calves are spotted at birth, but the spots fade after about two months.

The typical family group consists of a hind, a new calf, a yearling calf, and perhaps a two- or three-year-old stag. Mature stags and hinds live in separate groups for most of the year, with the hinds tending to monopolize the better, more grassy habitats. At the start of the mating season (the rut) in the early fall, the stags split up and join the females. Each eligible stag establishes a harem of up to 20 or more hinds, which he defends vigorously during the rut. During this period, which typically lasts 6–8 weeks, the stags often forego eating and lose as much as 15% of their body mass.

Red deer are one of the most widely distributed deer species: although they are native to Europe, today they can be found everywhere from New Zealand to North America. They are herbivores, feeding mainly on rough grasses, young tree shoots, and shrubs. Forest-dwellers by nature, they can adapt easily to different climates and terrain. In many of the areas in which they were introduced, red deer are commercially farmed for venison and antler velvet, which has been used in traditional Chinese medicine for over 2,000 years to treat a broad range of ailments, including anemia, arthritic pain and rheumatism, kidney disorders, and stress.

Darren Kelly was the production editor, and Audrey Doyle was the copyeditor for *Essential SNMP*, Second Edition. Carol Marti proofread the book. Genevieve d'Entremont and Colleen Gorman provided quality control. Lydia Onofrei provided production assistance. Johnna VanHoose Dinse wrote the index.

Ellie Volckhausen designed the cover of this book, based on a series design by Edie Freedman. The cover image is a 19th-century engraving from the Dover Pictorial Archive. Karen Montgomery produced the cover layout with Adobe InDesign CS using Adobe's ITC Garamond font.

David Futato designed the interior layout. This book was converted by Andrew Savikas to FrameMaker 5.5.6 with a format conversion tool created by Erik Ray, Jason McIntosh, Neil Walls, and Mike Sierra that uses Perl and XML technologies. The text font is Linotype Birka; the heading font is Adobe Myriad Condensed; and the code font is LucasFont's TheSans Mono Condensed. The illustrations that appear in the book were produced by Robert Romano, Jessamyn Read, and Lesley Borash using Macromedia FreeHand MX and Adobe Photoshop CS. The tip and warning icons were drawn by Christopher Bing. This colophon was written by Rachel Wheeler.