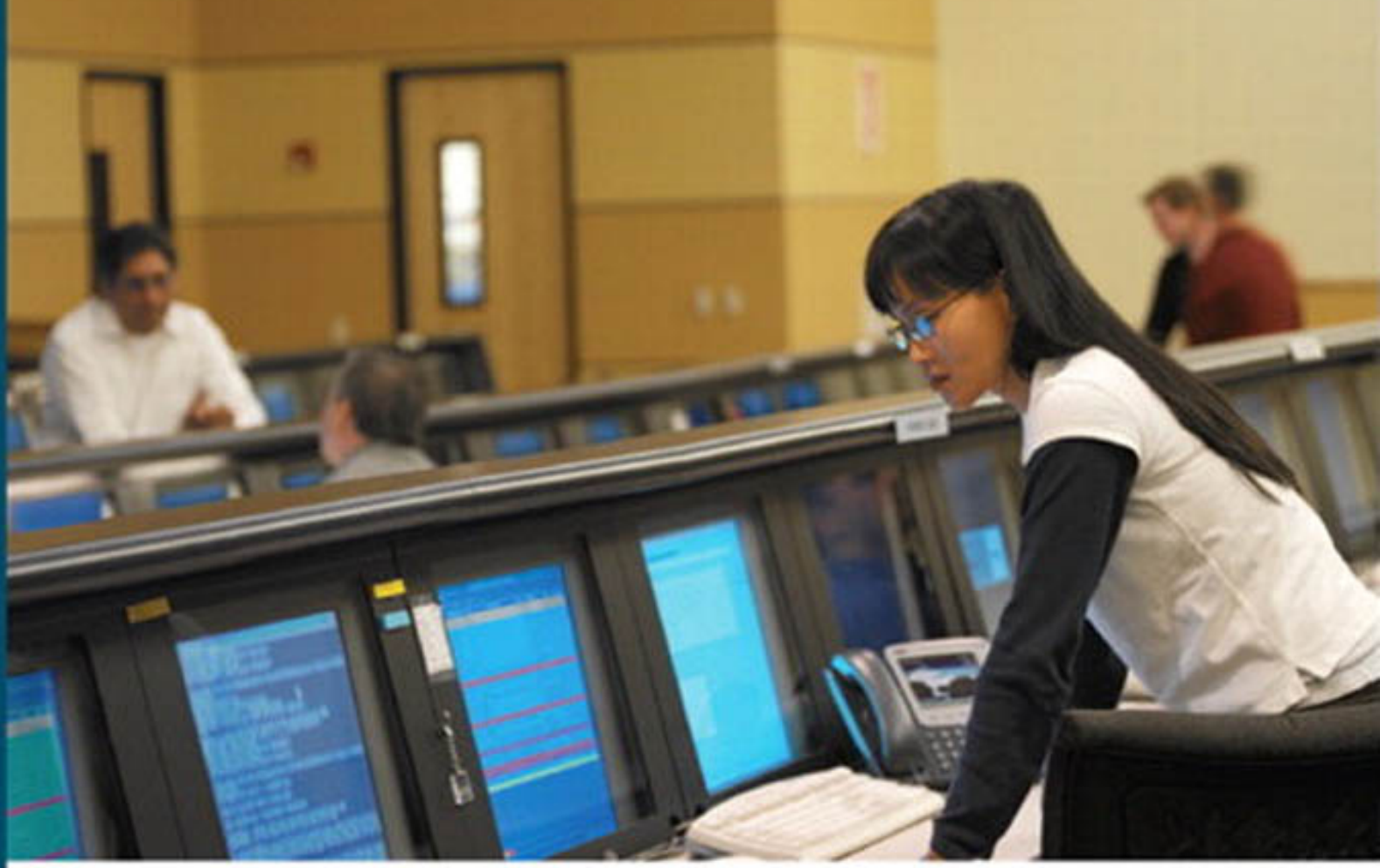
Network Management Fundamentals

A guide to understanding how network management technology really works



ciscopress.com

Alexander Clemm, Ph.D.

Network Management Fundamentals

Alexander Clemm, Ph.D.

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

First Printing November 2006

LIBRARY OF CONGRESS CATALOG CARD NUMBER: 2004110268

ISBN: 1-58720-137-2

Warning and Disclaimer

This book is designed to provide information about network management. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc., shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Corporate and Government Sales

Cisco Press offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact: **U.S. Corporate and Government Sales** 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside of the U.S. please contact: **International Sales** 1-317-581-3793 international@pearsontechgroup.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Publisher: Paul Boger
Executive Editor: Mary Beth Ray
Managing Editor: Patrick Kanouse
Development Editor: Betsey Henkels
Project Editor: Tonya Simpson
Copy Editor: Krista Hansing Editorial Services, Inc.
Team Coordinator: Vanessa Evans
Book and Cover Designer: Louisa Adair
Compositor: Mark Shirar
Indexer: Larry Sweazy

Cisco Representative: Anthony Wolfenden
Cisco Press Program Manager: Jeff Brady
Technical Editors: Prakash Bettadapur, David M. Kurtiak, Lundy Lewis

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

About the Author

Dr. Alexander Clemm, Ph.D. is a Senior Architect with Cisco Systems. He has been involved with integrated management of networked systems and services since 1990. Alex has provided technical leadership for many network management development and engineering efforts from original conception to delivery to the customer. They include management instrumentation of network devices, turnkey management solutions for packet telephony and managed services, and management systems for Voice over IP networks, broadband access networks, and provisioning of residential subscriber services. Alex has approximately 30 publications related to network management and 15 patents pending. He is on the Organizing Committee or Technical Program Committee of the major technical conferences in the field, including IM, NOMS, DSOM, IPOM, and MMNS, and he served as Technical Program Co-chair of the 2005 IFIP/IEEE International Symposium on Integrated Network Management. He holds a Ph.D. degree from the University of Munich and a Master's degree from Stanford University.

About the Technical Reviewers

Prakash Bettadapur is a Senior Engineering Manager at Cisco Systems. He has been with Cisco since 1999, working in various network management and IOS manageability programs. Before Cisco, Prakash worked in Bell Northern Research (BNR) in Ottawa, Canada, and in Nortel Networks in Santa Clara, California, for 14 years. While in BNR/Nortel, Prakash worked in DMS–Service Control Point, Data Packet Networking (DPN), Magellan Passport, and Meridian PBX product lines, focusing on the areas of software development and network management. Prakash holds a Master's degree in computing science from the University of Alberta, Canada; a Proficience Certificate in computing systems from the Indian Institute of Science, Bangalore; and a Bachelor's degree in electronics and telecommunications engineering from Karnataka Regional Engineering College, India. Prakash currently lives in San Jose, California.

David M. Kurtiak is a Principal Engineer for Loral Skynet, where he currently architects systems and network infrastructure and provides tier 3 support for the company's global IT organization. In a previous role at Skynet, Dave led a team of technical professionals responsible for managing the daily operations of the company's IT and data network infrastructure. Before joining Loral, Dave was a senior data communications specialist for AT&T. David has more than 18 years of experience in the IT and telecommunications industry, working in many telecommunications technologies. He is recognized as the resident expert in TCP/IP networking, with specialization in end-to-end network analysis, planning, troubleshooting, and performance tuning. David has a Master's degree (M.S.) in telecommunications from the University of Colorado at Boulder and a Bachelor's degree (B.S.) in information systems from the University of North Carolina at Greensboro.

Lundy Lewis is the Chair of the Department of Information Technology at Southern New Hampshire University. He has worked in the area of network management since the early 1990s. He holds 22 U.S. patents and has written three books on network and service management. He is a member of the technical committees for the major IEEE conferences on network management.

Dedications

To my wonderful wife and kids—Sigrid, Clarissa, and Christopher. Thank you for making me complete.

Acknowledgments

At various stages of writing this book, I had interesting discussions, support, and valuable feedback from many friends and colleagues. In particular, I would like to acknowledge Ron Biell, Steve Chang, Eva Krüger, Victor Lee, Dave McNamee, Fred Schindler, Hector Trevino, Eshwar Yedavalli, and Ralf Wolter. A very special "thank you" goes out to my dad, Helmut Clemm, who, in fact, read through the entire manuscript and, although not a "network manager," provided many useful insights.

I also want to acknowledge this book's production team, which is the finest anyone could ask for. Specifically, I would like to acknowledge the people I interacted with the most—Jim Schachterle, who first got the ball rolling; Raina Han and Mary Beth Ray, who accompanied me through most of the writing stage; and Betsey Henkels, whose development edits were of great help during the "crunch time" of the book; and Tonya Simpson, my project editor. The team also includes my technical editors, Prakash Bettadapur, David Kurtiak, and Lundy Lewis, whose excellent comments and suggestions undoubtedly helped to significantly improve the book.

Last but not least, I would like to thank my family for their understanding and support throughout this project, which, by the nature of things, meant sacrificing many weekends; nonetheless, they never stopped cheering me on. We did it!

This Book Is Safari Enabled

The Safari® Enabled icon on the cover of your favorite technology book means the book is available through Safari Bookshelf. When you buy this book, you get free access to the online edition for 45 days.

Safari Bookshelf is an electronic reference library that lets you easily search thousands of technical books, find code samples, download chapters, and access technical information whenever and wherever you need it.

To gain 45-day Safari Enabled access to this book:

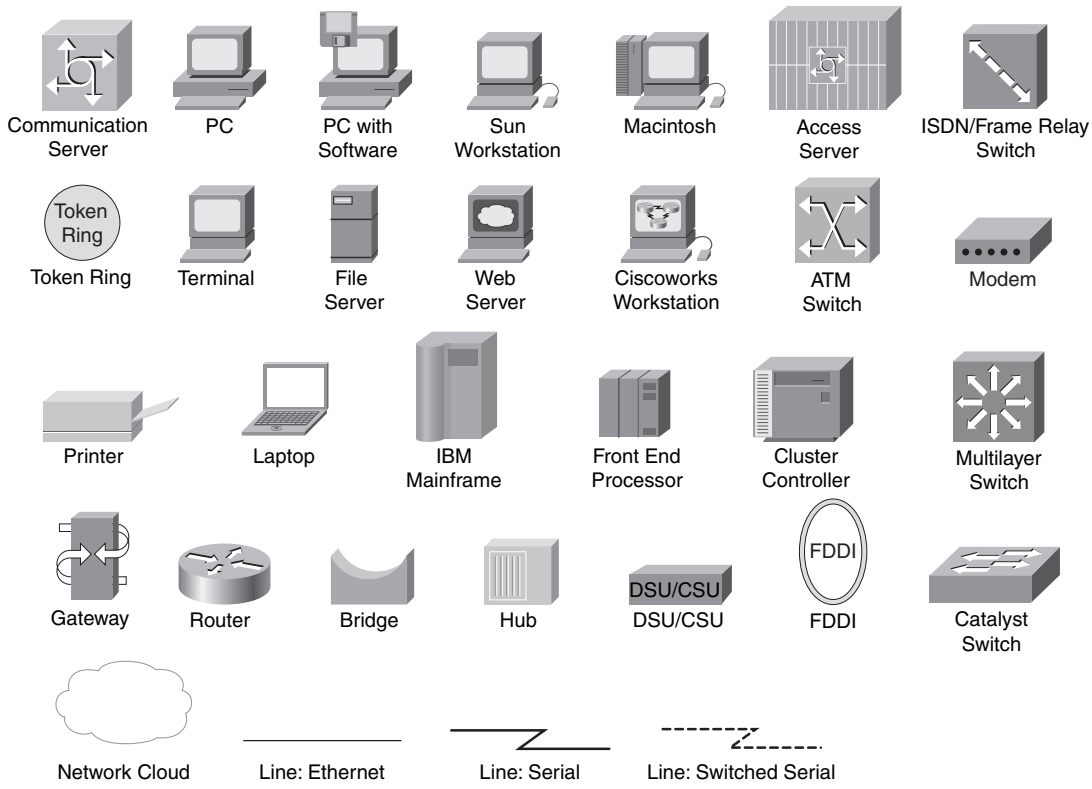
- Go to http://www.ciscopress.com/safarienabled

If you have difficulty registering on Safari Bookshelf or accessing the online edition, please e-mail customer-service@safaribooksonline.com.

Contents at a Glance

Contents

Icons Used in This Book



Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italics* indicate arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate optional elements.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

Network management is an essential factor in successfully operating a network. As businesses become increasingly dependent on networking services, keeping those services running becomes synonymous with keeping the business running.

Properly performed, network management ensures that services provided over a network are turned up swiftly and keep running smoothly. In addition, network management helps to keep networking cost and operational cost under control. It ensures that networking equipment is used effectively and deployed where it is needed the most. It increases the availability and quality of the services that the network provides. At least in the case of service providers, it is also a significant factor in the generation of revenue from networking services. On the other hand, ineffective management can lead to deterioration and disruption of networking services, poor utilization of investment made in the network, and lost business. Network management is hence key to getting the most value out of a network and can be absolutely business critical.

Despite its significance, network management is without much doubt one of the lesser understood topics in the otherwise well-charted world of networking. Reasons for this include the fact that network management looks deceptively simple, whereas it can be difficult to master, and that it is overshadowed by the networking technology itself that it is supposed to manage.

In some ways, managing a network is like throwing a party: Most people enjoy going to a party (read: the services provided by the network) but do not want to deal with the hassle of setting it up, keeping everything flowing smoothly, and cleaning up the mess afterward (read: network management). Yet this is essential to the party's success (and ensuring that there will be another one). As with network management, many technical disciplines are involved: Food needs to be cooked, rooms decorated, invitations printed, and electrical equipment and lighting set up. And as with network management, organizational and business questions abound: Do I throw it at my home, or do I lease a location? Where will I put the coats? How many drinks do I need? Can I do it all by myself, or at what point does it make sense to use a caterer?

Network Management Fundamentals aims to provide an accessible introduction to this important subject area. It covers management not just of networks themselves, but also of services running over those networks. It explains the fundamental concepts and principles that network management is based on. It attempts to provide a holistic system perspective of network management and explains how different technologies that are used in network management relate to each other. This system perspective aims to convey a sense of the forest rather than of the individual trees. Hopefully, the resulting understanding will put you, the reader, in a position in which you can successfully navigate the subject area of network management and apply its concepts to your particular situation.

Who Should Read This Book?

This book is intended as an introduction and guide to network management for anyone interested in the topic, whether that person has only a basic understanding of networking technology and is only casually interested in the subject, or whether that person is an experienced networking professional looking to expand his or her core competencies. The book tries to avoid overloading the reader with unnecessary complexity and details that would distract from these fundamentals and key concepts, yet provide a solid technical foundation for the practitioner.

The target audience includes network operators, development engineers, test engineers, operations planners, project managers, and product managers who need to deal with network management in some way as part of their jobs. It also includes executives who need to understand the impact of network management on their organization, as well as engineering students who want to round off a networking curriculum.

The emphasis in this book lies on fundamentals and general principles in network management rather than technical details and "how-to" instructions. Accordingly, if you are interested in the details of a particular management protocol or in the specifics of a particular management application, this is not the right book for you. If, on the other hand, you want to understand the foundations of network management and how management technology really works, this book should prove useful to you.

How This Book Is Organized

This book is intended to be read cover to cover because later chapters build on concepts and principles that earlier chapters introduce. Nevertheless, many chapters are relatively self-contained, which should make it fairly easy to move between chapters.

The chapters of this book are grouped into four parts:

- **Part I, "Network Management: An Overview,"** provides an overview of what network management is about and why it is relevant. It also conveys an informal understanding of the functions, tools, and activities that are associated with it. Part I consists of three chapters:

  Chapter 1, "Setting the Stage," provides an informal overview of what network management is all about, from both a business and technical perspective. It explains how one can benefit from network management and what basic challenges are associated with it.

  Chapter 2, "On the Job with a Network Manager," takes a glimpse at typical activities that people who run networks for a living are involved with, using three example scenarios. It also provides an overview of the types of tools they have at their disposal to support them in their jobs.

  Chapter 3, "The Basic Ingredients of Network Management," discusses the basic components in network management and the roles they play. This includes the network and the devices in it that need to be managed, the systems and applications that are used for their management, and the network that connects them for management purposes. It also includes the organization behind it that makes it all happen and that is ultimately held responsible for ensuring that the network is run properly.

- **Part II, "Management Perspectives,"** dissects the topic into its various aspects in a more systemic manner. In the tradition of the analogy of the elephant and the blind man, it illuminates network management from several different angles. This culminates in a discussion of how these aspects are combined into management reference models. Specifically, it includes the following chapters:

  Chapter 4, "The Dimensions of Management," presents different orthogonal (unrelated) yet complementary aspects in network management. An understanding of those aspects will help you divide and conquer network management problems that you might face. This includes different hierarchical levels of network management concerns, from dealing with equipment in the network to managing your business as it relates to networking. It includes the phases in the management lifecycle, from planning your network to decommissioning equipment. It includes the aspect of how to represent information about the managed network, how

managing and managed systems can communicate, and how to set up a management organization. Last but not least, it includes the management functions that are needed for network management in the first place.

Chapter 5, "Management Functions and Reference Models: Getting Organized," takes an in-depth look at the function dimension of network management—specifically, the range of different functions that management systems need to cover. It proceeds along the lines of several well-established *management reference models*, such as the FCAPS model, that do an excellent job of organizing these functions.

- **Part III, "Management Building Blocks,"** dives further into different building blocks of network management, picking up on various aspects encountered in conjunction with the management dimensions that Part II introduces.

  Chapter 6, "Management Information: What Management Conversations Are All About," discusses what lies at the core of all communication between managing and managed systems—namely, how to establish a common understanding of what is being managed and different ways to represent this information for management—how it is modeled, how it is represented (for example, as part of a Management Information Base), and how it is encoded over the wire.

  Chapter 7, "Management Communication Patterns—Rules of Conversation," dives into the various patterns in which managing and managed systems interact. These patterns have a profound impact on many areas, from how management communication protocols are designed to how management applications are architected so they can scale.

  Chapter 8, "Common Management Protocols: Languages of Management," presents a sampling of what are arguably the most important and widely deployed management protocols today—in effect, languages that managing and managed systems use to communicate with each other and exchange management requests, responses, and event messages. The technologies presented include SNMP, CLI, syslog, Netconf, and NetFlow/IPFIX. In addition to a technical overview, the chapter also explains how they are positioned with regard to the management purposes they serve and what their most important distinguishing characteristics are.

  Chapter 9, "Management Organization: Dividing the Labor," takes a closer look at the different ways in which management can be organized from a technical perspective and how management functionality can be divided between different systems. In particular, it explores the "vertical" division of management tasks in which different systems need to collaborate to ultimately achieve a common management purpose.

- **Part IV, "Applied Network Management,"** rounds out the book with a number of management topics of general interest. These topics also combine and put into perspective many of the pieces that were introduced earlier.

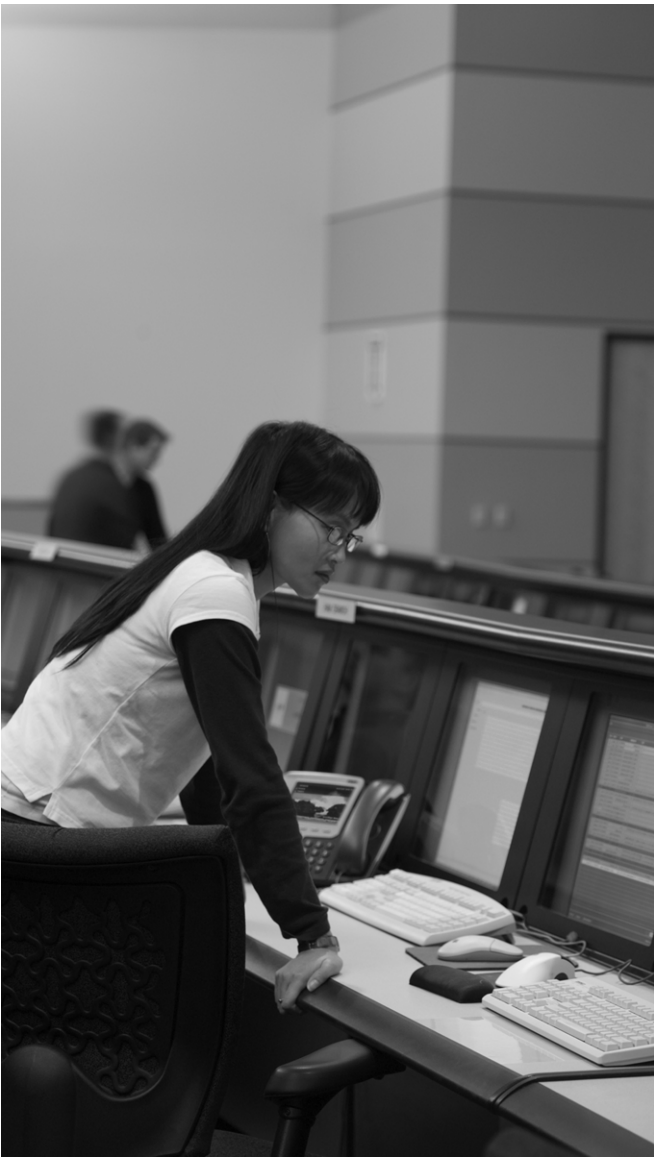
  Chapter 10, "Management Integration: Putting the Pieces Together," explores what is considered by many the "Holy Grail" of network management—namely, how to achieve management that is *integrated* and that provides all management functionality in a holistic fashion. The goal of this is to avoid the shortcomings and inefficiencies of management that is provided in the form of multiple islands. The chapter discusses the challenges that are associated with integrated management; articulating what those challenges are is the first step in confronting them successfully. Subsequently, the chapter presents techniques for tackling those challenges, along with their tradeoffs.

  Chapter 11, "Service Level Management: Knowing What You Pay For," presents an introduction to service level management. This topic is of fundamental importance, both to the providers of networking services, who need to ensure that agreed-to service levels are being met, and to their customers, who want to validate that they are indeed getting the level of service they pay for. It also serves as an example of a practical management application area that puts to use many of the concepts that were introduced earlier in the book.

  Chapter 12, "Management Metrics: Assessing Management Impact and Effectiveness," revisits the business proposition of network management that the Introduction initially laid out. It thus closes a circle and provides a fitting conclusion for the book. The chapter examines what factors determine the effectiveness and impact of network management. It also shows how an assessment of network management impact and effectiveness can be methodically approached through use of metrics.

This page intentionally left blank

Part I: Network Management: An Overview



CHAPTER 1

Setting the Stage

This chapter sets the stage for the rest of the book. It provides an overview of what network management is all about, how you can benefit from it, and what basic challenges are associated with it. Don't worry—the chapters that follow provide you with a solid foundation to successfully deal with many of those challenges. This chapter gives you the background necessary to understand the remainder of this book and, in general, put you in a network management frame of mind.

After reading this chapter, you should be able to:

- Explain the term *network management*
- Develop a basic sense of what is involved in network management
- Explain the importance of network management and how it impacts cost, revenue, and network availability
- Recognize the different players and industries that have an interest in network management, and understand the different angles from which they approach the subject
- Describe some of the challenges posed by network management, including those that are technical, organizational, and business

Defining Network Management

As is the case with so many words, *network management* has many attached meanings. Therefore, some clarification is in order regarding what is meant by the term in this book.

Speaking informally, *network management* refers to the activities associated with running a network, along with the technology required to support those activities. A significant part of running a network is simply monitoring it to understand what is going on, but there are also other aspects.

What network management is all about is perhaps best conveyed using some simple analogies.

Analogy 1: Health Care—the Network, Your Number One Patient

A network is not unlike a complex living organism. Let us therefore compare a network with a patient who is in an intensive care unit in a hospital. The patient, of course, is under intensive scrutiny, just as your network should be. After all, the network could be the lifeblood of your enterprise.

In an intensive care unit, monitoring the patient's pulse is constantly required. A slowing or missing pulse, after all, requires an immediate response. Other health functions of the patient are monitored as well, such as temperature and blood pressure. Because they do not require as constant attention as the pulse, it is sufficient to measure them only once an hour or so. Curves are often plotted to detect trends over time, to answer not just questions such as "What is the patient's current temperature?", but also questions such as "Is the temperature dropping or rising?" In addition, on a more exceptional basis, blood samples are taken and analyzed, and under special circumstances an MRI is performed.

In response to the patient's symptoms, doctors prescribe a set of medications and treatments. Again, through monitoring, the patient's response is observed and diagnoses are confirmed or alternative paths of treatment are considered if the response is different than expected. Needless to say, an extensive hospital staff, expensive equipment, and millions in R&D dollars to develop effective drugs are required to provide the best possible care for the intensive care patient.

Likewise, a network must be monitored. In fact, people often refer to the "network health" when they are discussing network performance and its capability to provide service. As with the pulse of a patient, critical functions of network equipment that could lead to service outages need to be monitored constantly and malfunctions alarmed immediately to react as quickly as possible when trouble occurs. As with the temperature or blood pressure of a patient, other parameters could be indicators of impending trouble, such as increasing rates at which packets are dropped or utilization on a link that is approaching 100 percent. These parameters must be closely monitored, and changes and trends must be heeded. For example, a rising packet-drop rate could be an indication of impending failures, whereas rising link utilization could be an indication that additional network capacity is required.

Under certain circumstances, extensive troubleshooting and diagnostic procedures must be run. Some of those procedures can be costly because they require, for example, that network devices spend precious cycles running diagnostics instead of routing packets, or because, in extreme cases, a device or a port must be taken offline to run a test. Therefore, those functions would not be run constantly, but only when called for, just as special circumstances are required to run an MRI on a hospital patient.

To remedy failures and react to signs of trouble, networking parameters must be tuned and devices might need to be reconfigured—in some cases, even replaced. This is the equivalent of "medicine"

for the network. The effect of the actions taken is again monitored to ensure that the desired result is reached; otherwise, alternative methods of treatment are attempted. And as with the hospital patient, effective organization and management tools are all required to keep things running smoothly.

Analogy 2: Throwing a Party

Running a network has much in common with running events. Think for a moment of a network as analogous to a big party—not a party you attend as a guest (that is, an end user), but one that you are hosting (that is, managing).

Depending on the type of party and the number of guests, throwing a party involves many different activities. Long before the date of the party, planning begins: Invitations need to be designed, printed, and sent out. Organizational questions abound. Do you throw it at your home, or should you rent a spot at another location (and which one)? What external circumstances do you need to consider? Depending on the season and where you live, you might need to think about where to put the coats. Food must be prepared and rooms decorated. You need to decide whether to throw the party all by yourself or at what point you would rather use a caterer. Of course, it is also a question of money. How many drinks will you need? You don't want to run out, but on the other hand, you don't want to be wasteful by serving too much. Electrical equipment and lighting need to be set up. During the party, you want to make sure your guests are feeling comfortable. Do you need to bring more drinks? Is the volume of the music at the right level? Finally, after the party, there is the cleanup to take care of.

Likewise, many activities are involved with running a network. As in the case of the party, you begin with planning: What services do you intend to provide over your network, and what service capacity will be needed? What circumstances will influence your network topology—for example, do you need to connect many small branch offices, or are you planning a network for one large campus? The answer likely influences the choice of equipment and dimensioning of links. Equipment, in turn, must be commissioned and turned up. In many cases, special configuration activities and tuning of configuration parameters might be required—not an easy feat, given the multitude of knobs that can be turned, the technical interdependencies, and the many different types and versions of equipment in the network.

Business questions need to be answered as well. Should you use the equivalent of a caterer and simply buy a set of communication services and outsource operation of the network, or should you manage your own network? Do you have the expertise to do so? Budget might be limited, forcing you to make hard choices. Furthermore, unlike throwing a party, the task of running the network never ends. This complicates matters further. You need to be able to continually make adjustments as you go and introduce new services. You might need to decommission and replace old equipment without affecting end users. And, of course, all along you need to make sure that everything is

functioning properly so that the end users of your communication services will be happy, just as you want the guests at your party to feel comfortable.

A More Formal Definition

Given the previous examples, this definition sums up a little more formally what's involved in managing a network:

> Network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems.

Operation deals with keeping the network (and the services that the network provides) up and running smoothly. It includes monitoring the network to spot problems as soon as possible, ideally before a user is affected.

Administration involves keeping track of resources in the network and how they are assigned. It deals with all the "housekeeping" that is necessary to keep things under control.

Maintenance is concerned with performing repairs and upgrades—for example, when a line card must be replaced, when a router needs a new operating system image with a patch, when a new switch is added to the network. Maintenance also involves corrective and preventive proactive measures such as adjusting device parameters as needed and generally intervening as needed to make the managed network run "better."

Provisioning is concerned with configuring resources in the network to support a given service. For example, this might include setting up the network so that a new customer can receive voice service.

The following figures illustrate the role that network management plays. Figure 1-1 depicts the task of running and monitoring a network that the organization responsible for the network is faced with. Figure 1-2 depicts where network management fits in to help organizations responsible for managing a network with their task. Figure 1-3 depicts what is included in network management—namely, the systems and applications used to manage networks, as well as the activities and operational procedures that those systems support.

Figure 1-1 *An Organization and Its Network*

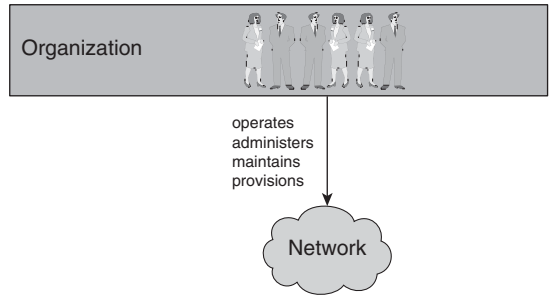


Figure 1-2 *The Role of Network Management*

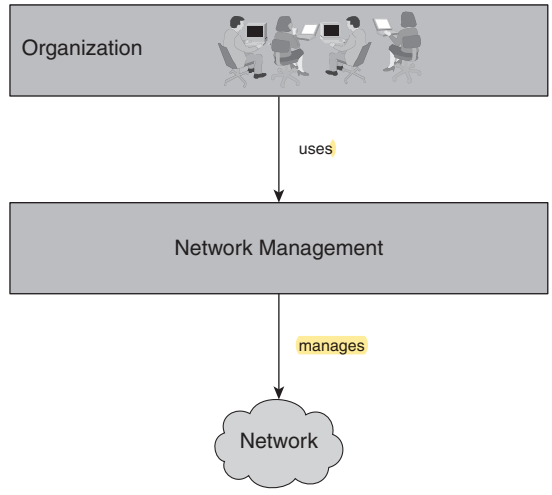
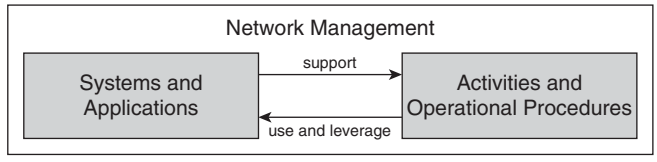


Figure 1-3 *What Constitutes Network Management*

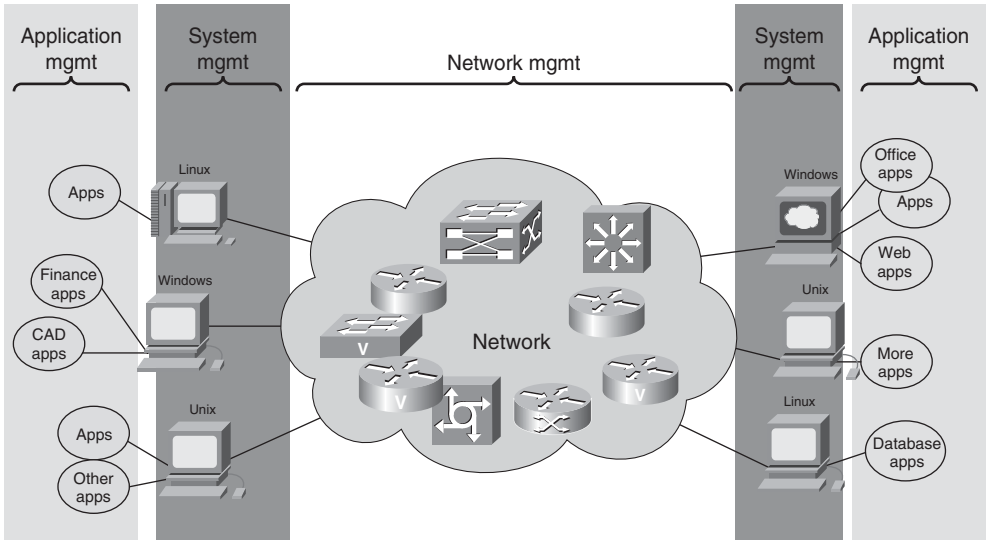


A narrower definition of network management would not refer to "networked systems" in its generality, but simply to "communication networks." Sometimes a distinction is made among the management of the networks themselves, the management of the end systems that are connected to networks, and the management of (networked) applications running on the systems connected to the networks. This distinction separates the terms *network management*, *systems management*,

and *application management*, as depicted in Figure 1-4. In addition, networks, systems, and applications might all be involved in providing a service. Management of the service is therefore often distinguished as well and subsumed under the term *service management*.

Although there are certainly specifics to each of those management disciplines, they have much more in common than what separates them. Unless otherwise noted, we use the term *network management* in its broader sense, encompassing all of these very closely related disciplines.

Figure 1-4 *Network, Systems, and Application Management*



The Importance of Network Management: Many Reasons to Care

Wouldn't it be nice if, to run a network, you just had to buy a bunch of networking equipment, wire it and hook it up, flip a switch, and, voilà—the network just works. You can turn off the lights and basically forget about it and simply enjoy the services that it provides, kind of like an entertainment center in a living room. Well, although you might wish it were that simple, you can't quite get away with so little effort.

A network is a complex structure that requires a great deal of attention. It must be carefully planned. Configurations of network devices must be modified without adversely affecting the rest of the network. Failures in the network do occur and need to be detected, diagnosed, and repaired. Service levels that were guaranteed to customers and end users—for example, a certain amount of bandwidth—need to be monitored and ensured. The rollout of services to customers and end

users—making service offerings available to them and turning up services quickly when they are requested—must be managed.

Many telecommunications and Internet service providers (ISPs) are finding that the communication services they offer—long-distance telephone service, Internet access, digital subscriber line (DSL)—are becoming commoditized. As a consequence, in many cases not only the base offering itself determines success or failure in the marketplace. Other factors are becoming increasingly important:

- Who can operate the network at the lowest cost and pass those cost savings on to customers?
- Who provides better customer experience by making it easy to order communication services and service those orders with minimal turnaround time?
- Who can maintain and guarantee the highest quality of service?
- Who can roll out services fast and efficiently?

Operating a network is hence truly at the core of the business for service providers. (Service providers are sometimes also referred to as *network operators*. However, we prefer to use the term *operator* for personnel who operate and maintain the network, not for the organization that they are part of.)

Similar factors apply to businesses and enterprises that run their own networks: Cost savings in operating the network benefit the enterprise that the network serves; fast turnaround time to deploy new services and maintain a high quality of service can translate into important competitive advantages. All these factors are ultimately economic success factors, and they are all intricately linked to network management. Therefore, network management is a key factor for the economics of running a network. The significance of network management to that regard cannot be overemphasized.

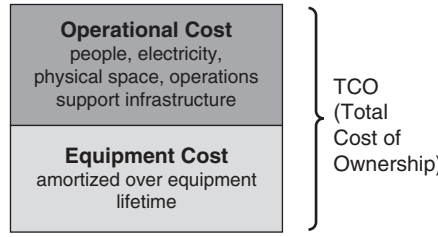
This section provides a closer look at the benefits that effective network management and management tools can provide—reduced cost, improvements in the quality of service that the network provides, and increased revenue. From now on, we refer to the organization that is running a network simply as the *network provider.* In some cases, we also use the term *service provider* in reference to the services that those organizations provide over the network. Unless mentioned otherwise, we do not limit use of the term to "classical" service providers such as telecommunications carriers or Internet service providers, but we include also enterprise IT organizations. After all, they provide communication services to the enterprise that they are part of.

Cost

One of the main goals of network management is to make operations more efficient and operators more productive. The ultimate goal is to reduce and minimize the total cost of ownership (TCO) that is associated with the network. The TCO consists essentially of the equipment cost, as well as the cost to operate the network (see Figure 1-5). Equipment cost is typically amortized over several years, to take into account the lifetime of the equipment. Operational cost includes cost such as operating personnel, electricity, physical space, and cost for the operations support infrastructure.

The cost savings that result from a lower TCO make the service provider more competitive from an economics perspective. In addition, the service provider can pass the cost savings on to its customers, thus making them more competitive. The expectation is that network management can help accomplish this.

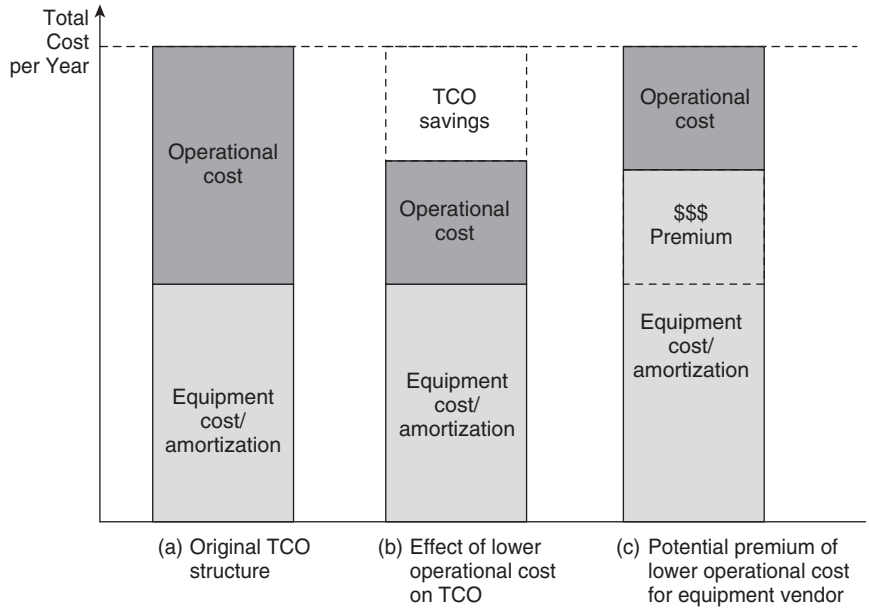
Figure 1-5 *Total Cost of Network Equipment Ownership*



To put things in perspective, the cost of operations can be higher than the cost of amortizing the network equipment itself, in some cases by as much as a factor of 2 or more. To illustrate, assume for a moment that an equipment vendor charges $300,000 for a set of network devices, which are amortized at $100,000 per year over 3 years. Assume furthermore that for a given service provider, the associated operational cost is an additional $200,000 annualized.

From a service provider perspective, a competitor who manages to realize an operational efficiency gain of 25 percent will enjoy a competitive cost advantage of $50,000 per year, or half the entire equipment amortization cost. From an equipment vendor perspective, a vendor whose management capabilities result in a mere 25 percent operational efficiency gain will be capable of charging 50 percent more for equipment as a premium for its superior operations capabilities, or $150,000 instead of $100,000, at the same TCO. Figure 1-6 illustrates this fact. (Unfortunately, it is not always easy to come up with definitive numbers for TCO and crisp models for return on investment on network management. Chapter 12, "Management Metrics: Assessing Management Impact and Effectiveness," presents more information on how management effectiveness can be assessed and translated into monetary values.)

Figure 1-6 *The Significance of Lowering Network Equipment Operational Cost*



The following are examples of how the application of network management tools can help increase operational efficiency and lower cost:

- Network testing and troubleshooting tools. These tools enable operators to more quickly identify and isolate problems and thereby free themselves up for other tasks. Automating troubleshooting for routine problems enables operations personnel to focus on the really "tough" issues.
- Systems that facilitate turn-up of services and automate provisioning. By automating most of the steps that are required to enable a service for an end user, fewer operational steps must be performed by an operator. This also reduces the potential for human error.
- Performance-reporting tools and bottleneck analysis. This enables service providers to allocate network resources to where they are needed most, minimizing the required investment in the network and maximizing the "bang for the buck."

Another cost benefit of network management tools, besides operator productivity, is that such tools potentially reduce the skill level that is required to manage the network. This reduces investment in training. It also increases the pool of qualified labor that is available, making hard-to-find skill sets less of a bottleneck and limiting factor in the service provider's business. One of the most critical hurdles in operating a network—and, therefore, an incentive to increasing

efficiency—is that, in many cases, it might simply not be possible to hire and train sufficient numbers of skilled engineers.

Quality

Other operational aspects are not related to cost but are equally important. One such aspect concerns the quality of the communications and networking services that are provided. This includes properties such as the bandwidth that is effectively available, or the delay in the network, which, in turn, is a factor in the responsiveness a user experiences when using services over a network.

Quality also includes the reliability and the availability of a communications service: As an end user, can I rely on my service, or do I need to often retransmit data because I experience interruptions in the middle of my communication session, such as timeouts and no response from the remote end because of a dropped communication session? Is the service always available when I need it, or do I sometimes (in the case of voice service) get no dial tone? Availability is not simply nice to have; lives can literally depend on it. For example, think of a 911 service in a telephone network, or connectivity for critical equipment in a hospital.

Reliability and availability are attributes that are typically associated only with the network itself. Accordingly, and rightfully so, much emphasis is given to engineering networks in a way that makes them carrier class. This involves developing network equipment with redundant hardware so that if a component fails, a hot failover to a spare can occur. In addition, networks themselves are carefully engineered to allow for redundant communication paths, in many cases ensuring network availability that is overall higher than the availability of any single element in the network. Intelligent capabilities are introduced to automatically reroute communication traffic around faults or fiber cuts. The list goes on.

One aspect that is easily overlooked, however, is the fact that network management is also a key ingredient in this equation. Here are some examples:

- Systems for the end-to-end provisioning of a service automate many of the steps that need to be performed to configure the devices in the network properly. Those systems help make operations not only more efficient, but less error prone as well because they provide fewer opportunities to make mistakes. Misconfigurations, in which some devices or network parameters are not set up properly, result in lower network and service availability. They can be hard to troubleshoot and slow to fix. Through end-to-end provisioning, many such misconfigurations can be avoided in the first place, providing an important contribution to increased network availability.

- Performance trend analysis can help network managers detect potential network bottlenecks and take preventive maintenance action before problems occur and before services and users are negatively impacted. This can also help improve the level of service being delivered, such as the bandwidth that is effectively available to users or delay that is introduced in the network.
- Alarm correlation capabilities enable faster identification of the root cause of observed failures when they occur, minimizing the time of actual outages.

Even more than with cost, it is difficult to quantify the return on investment in network management with respect to quality. One possibility is to consider opportunity cost, the cost if quality is *not* met. Examples for opportunity cost are listed here:

- Lost revenue from customers taking their business elsewhere if quality objectives are not met.
- Increased networking cost from inefficient utilization or networking resources, which potentially leads to more networking equipment and capacity being deployed to support a certain level of service than would otherwise be necessary. This results in higher equipment cost and a larger footprint—for example, space for all that equipment.
- Higher operational cost that is spent on fixing problems and having to monitor additional equipment that would not be necessary if quality would meet required levels and existing equipment were better utilized.

Revenue

Network management is not just related to cost and quality. Network management can also be a revenue enabler that opens up market opportunities that would not exist without it. Here are some examples:

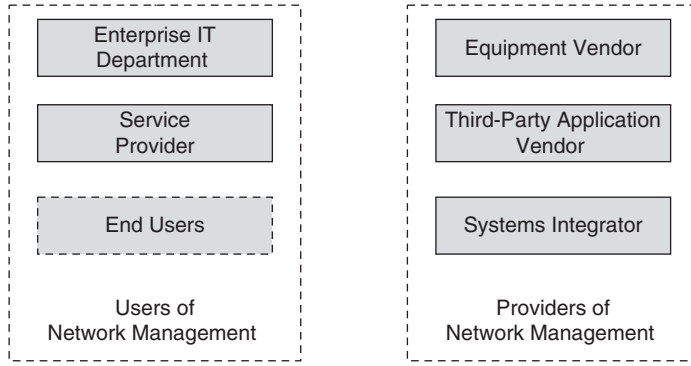
- Service provisioning systems enable service providers to reduce the time that elapses from the time a service is ordered to the time the service is actually turned up. The capability to turn up a service quickly translates into quicker time to revenue generation. A management system that automates the complete workflow, from ordering the service to turning it up, obviously provides greater speed than workflows that involve human operators who need to key data into multiple systems redundantly along various steps of the way. Also, if a service cannot be provisioned and turned up quickly, a customer might decide to take his business elsewhere.
- In some cases, network management enables a service provider to augment a service offering with management-related capabilities that attract more customers. For example, to a customer, the capability to track accounting charges online and to configure service features over the Web (examples for voice: caller ID, follow-me services) and have them take effect immediately constitutes a valuable service feature.

- Cost savings made possible through network management might make certain services feasible in the first place. For instance, a new communications service for residential customers might not be feasible if it takes several hundred dollars in operational cost per subscriber just to turn up that service. Residential customers might not be willing to pay such amounts, and service providers might not be willing or able to absorb them. (This is what happened in the early days of digital subscriber line [DSL] service, for example.) An efficient management system that reduces or eliminates truck rolls might be the prerequisite to economically offer a service in the first place and open up a whole new market. (A truck roll refers to the need to send operations personnel to a customer site, which typically involves "rolling a truck" and is associated with high cost.)

The Players: Different Parties with an Interest in Network Management

Network management is a whole industry that involves many players. Different players are concerned with different aspects of network management, depending on their particular perspective. In this section, you learn who the players are and what role network management plays for them. Roughly, the players fall into the categories of users of network management and providers of network management (see Figure 1-7).

Figure 1-7 *Players in the Network Management Space*



Network Management Users

The Service Provider

As their name indicates, service providers are in the business of providing services to their customers. Those services can be any communication and networking service, such as telecommunication services (telephone, voice mail) and data services (leased lines, Internet

connectivity). In some cases, service providers host applications—they are then also called application service providers.

Many different types of service providers exist, categorized along different criteria—for example, according to what services they provide (telecommunications service providers, Internet service providers, application service providers, and so forth) or whether they are regulated by government (regulated incumbent service providers; local exchange carriers; Post, Telegraph, and Telephone administrations [PTTs]; or unregulated "competitive" local exchange carriers).

What all those service providers have in common is that they make a living out of running networks—running networks is the core of their business, their sole purpose of existence. Network management is accordingly of existential importance to them—and they are not interested in it just for its cost-saving potential, although, of course, given their massive operations, they also need to keep cost at bay. Even more important, service providers are interested in network management as a guarantor for their revenues. How they manage their networks is a key competitive differentiator. In particular, in an environment where many communication services are being commoditized (basically, anybody can offer long-distance voice service or a connection to the Internet), other factors make or break a service provider—and many of those factors are directly related to network management. Again, the winner in the marketplace is the service provider that can turn up services and roll them out to customers the fastest, that can offer the best service level guarantees, that knows how to be the quickest to recover from failures and how to limit their impact to a minimum, and that can best utilize its equipment and get the most mileage out of it. Because it is of such utmost importance, service providers are willing to invest heavily in network management—in development of efficient operational procedures to give them the upper hand, and in custom tools that best support those procedures.

The Enterprise IT Department

Enterprise IT departments are in charge of running the network inside an enterprise, providing the enterprise with all its internal communication needs. They are often thought of as mini service providers of communications services for the enterprise that they are part of. Although this is correct, some important differences exist:

- Generating revenue and making money are not important for the enterprise IT department. Instead, it is essentially a cost center, so the focus is on how to provide the communication services the enterprise needs at the lowest cost possible. Enterprise IT departments don't generate revenue; to some degree, they might be concerned with making sure enterprise departments get charged for their consumption of communication services, but, in many cases, this not a critical function. Not so for the service provider: It provides communications services for a living, so making sure that dollars are charged and collected is top priority.

- Enterprise IT departments have one customer: the enterprise. End users within the enterprise have no choice in who provides their service. (Of course, enterprises might choose to outsource many or most of their communication services to a service provider, again, to control cost.) Likewise, the enterprise IT department couldn't attract customers from outside the enterprise even if it wanted to. Service providers, on the other hand, have many customers, and those customers do have a choice. This puts a different emphasis on how customer relationships are managed and tied into operations.

- Because communications services are not the core business of the enterprise, how to manage and run their networks is not a primary competitive differentiator. In fact, enterprise IT departments might be forced to outsource much of their operations to a service provider (then called a managed service provider), to minimize distraction for the enterprise from their core business.

- Enterprise IT departments are not regulated, whereas, in many cases, service providers are. (However, the adoption of Sarbanes-Oxley legislation in the United States is changing that and, in fact, does have a certain regulatory effect on enterprise IT departments.)

Interestingly, network size isn't really a defining difference. Although it is true that the largest networks are owned by service providers, some very large enterprises—in particular, global Fortune 500 companies—own networks that, in size, number of end users, and communications volume, are on par with and, in many cases, even larger than those of many service providers.

Because network management, while important, isn't as differentiating and as critical a factor for large enterprises as it is for service providers, the investment in management applications and tools might be more restrained. The enterprise might be more willing to settle for generic applications and standard tools to save cost. It generally avoids investing in expensive custom network management development when possible.

The End User

Finally, there is the end user. With end users, here we are referring not to the users of the communication service—to them, network management is invisible; it is simply part of the infrastructure that keeps it all running. We are instead referring to the persons who keep the network running—the network managers. They are the ones who are ultimately the users of the various management systems and applications, and who rely on them as tools to get their jobs done. Collectively, network managers are often also referred to as operators, although, in fact, many different responsibilities and roles can be differentiated, depending on the organization. These roles include network administrators who can configure and tune routers and switches remotely, and who know how to troubleshoot the network when things aren't going right. They include the craft technicians, who are dispatched to fix problems that can't be fixed remotely, or to commission and decommission equipment. They include the help-desk representatives, who take user calls and complaints, and support personnel, who monitor the network. They include the network planners

who design the network, plan the topology, dimension links and nodes, and select the network equipment.

In fact, the roles of network managers vary greatly, depending on the organization. In the cases of smaller enterprises, the same person might be responsible for it all and wear many different hats, being a very sophisticated Jack-of-all-trades. In the case of large service providers, an entire army of personnel might be involved in running the network, which results in much greater specialization and myriad roles and job descriptions.

Network Management Providers

The Equipment Vendor

Equipment vendors are primarily in the business of selling networking equipment, not network management applications. Hence, traditionally equipment vendors have shown a tendency to limit investment in management application development. In general, they have been willing to settle for the minimum management capabilities that customers would allow them to get away with. That means that generally they would provide just the level of management capabilities needed to not inhibit equipment sales. Of course, they might have heard an occasional complaint as a result. However, if at the end of the day the vast majority of their customers made their purchasing decisions based on the capabilities of the equipment, not the management that comes with it, and if on top of that many customers expected any management capabilities to be thrown in essentially as a freebie without being charged extra, who could blame them?

In recent years, however, a subtle shift has started to occur in which people think of networking equipment less in terms of "boxes," but more in terms of end-to-end systems. Management, while not a part of the box, is certainly a part of that system. At the same time, there is an increasing awareness that TCO of a network includes not only the cost of buying or leasing the equipment, but the cost of managing it as well. Increasingly, that total cost is being factored into purchasing decisions. In addition, equipment vendors face constant pressure to avoid commoditization of their equipment. If everyone offers the same basic set of features, it becomes hard for vendors to charge a premium for their equipment, and margins suffer. On the other hand, when a particular vendor's equipment offers additional features and functions that are useful to end customers and that the competition doesn't have, this constitutes a positive competitive differentiator that the vendor might even be able to charge a premium for.

The capability to manage networking equipment is therefore increasingly being recognized as one such competitive differentiator. Hence, equipment vendors are paying increasing attention to network management. This includes management applications that equipment vendors make available for the equipment. In some cases, basic management software might come bundled with the equipment, not unlike a vendor of digital cameras that throws in additional photo-editing

software. But at least as important, this also includes the management interfaces of the equipment that allow the equipment to be easily supported by management applications and to be easily integrated into operations support environments.

The Third-Party Application Vendor

Third-party management software application vendors fill the management application gap that equipment vendors leave open. For one, management application software developed by an equipment vendor tends to support only equipment of that particular vendor. Even if multivendor support is provided, preferential treatment is given to the vendor's own equipment, in terms of both available features and the timeline at which the support becomes available. At the same time, as stated previously, in some cases management application software provided by equipment vendors delivers merely the minimum functionality that is required to keep network management from becoming a deal-breaker for equipment sales. The result in those cases is not always the best possible application.

In addition, many network providers have management needs that are not tied as much to any particular equipment in the network, but to operational tasks and workflows. In addition, many management needs are related to the particular communication services that network providers supply on top of the equipment to their own customers. Because those aspects are more removed from the equipment itself, the equipment vendor is less likely to be able to help network providers with those aspects.

This provides an opening that independent (third-party) management software application vendors are trying to fill. For simplicity, we refer to those vendors simply as management vendors. Management vendors try to make a living of selling management software. They have to make money from it and, therefore, charge a premium. In return, they need to offer features that network providers—service providers and enterprise IT departments—will be willing to pay for. Often one of those features is vendor independence—or perhaps, more precisely, multivendor support, meaning that the application will work well across equipment from different vendors.

The Systems Integrator

Organizations that run large networks, whether enterprise IT departments or service providers, eventually find that no one tool or application can do it all. Instead, over time they end up with a multitude of applications for different purposes. Nevertheless, the applications must, at least to a certain degree, be integrated with the overall operations support environment. They might have to operate from the same set of data—for example, inventory data of the network. They must be tied into the same workflow and many of the same procedures. Also, they must manage different aspects of the same network. Unfortunately (or fortunately, if you are a systems integrator), things don't always work together as seamlessly out of the box as the network provider would like. In addition, in many cases, network providers need additional pieces of functionality, tailored to their

specific needs, that their management systems do not provide and that they cannot buy from an independent management vendor.

This is where the systems integrator comes in. Systems integrators provide services to integrate a set of management applications with a specific network and operations support environment, often plugging functional gaps and providing interface adaptations that might be necessary to turn a set of independent applications into a turnkey solution that is customized for a specific network provider. So, like the management vendor, the systems integrator makes a living from network management. However, unlike management vendors that aim to make an off-the-shelf product of management applications that they can sell to multiple network providers, the systems integrator performs custom-tailored development.

Network Management Complexities: From Afterthought to Key Topic

A little earlier, we compared network management to running a big party. This analogy is actually appropriate in more ways than one: When deciding to throw a party, no one thinks at first of the effort that goes into planning the party, the logistics, the cleanup—you think of the party itself and how much everyone will enjoy it. And certainly no one throws a party just for the sake of the work that it involves, but for the fun they expect out of it.

This is not unlike the situation with networking and network management. When you first set out to deploy a network, chances are, at the center of attention initially is the network itself and the communication services that it provides, not how to run it. Network management is little more than an afterthought at first. One thing is sure: No one deals with network management just for network management's sake.

However, as the complexity of your network increases, so does the relevance of network management. More devices are added. Different types of devices are introduced, and different versions of the same type of equipment start to appear. At the same time, more users get connected to the network and use an ever-greater variety of communication services. You will soon find that it is hard to keep up with all that. In fact, the number of new users to add and new services to introduce might start to outpace your capability to do so.

Eventually, things start to break—they are not supposed to, but once in a while, they do. Even worse, you don't even realize it initially until some of the users on your network start complaining. Now you are quickly starting to become really overwhelmed.

At the same time, your competition seems to have a better handle on their network. Their network is utilized better; they accomplish more with less. This helps keep their cost down, while yours is spinning out of control. They can turn up new services for their users faster and more quickly reap

their benefits, while you have trouble just keeping things running as they are. Suddenly, it becomes strikingly clear to you that network management is much more than an afterthought. It is, in fact, the key topic. It is the difference between the network running you and you running the network, between failure and success, between tailgating with a six-pack in a parking lot (not that this wouldn't be some fun once in a while, too) and feasting at an elegant restaurant.

This is the type of experience for quite a few organizations that run networks. The sudden realization of its importance eventually moves network management to the center of attention as far as the communications infrastructure is concerned. At the same time, it becomes quickly clear that network management isn't really that trivial after all. Indeed, it comes with plenty of challenges that are interesting, exciting, and very rewarding to deal with. The sections that follow are intended to illustrate where some of those challenges lie. Developing a sense of those challenges is important for a number of reasons:

- It implies a sense of what the underlying problem domain is all about. Therefore, it is an important prerequisite for its understanding.
- It is a key to dealing with those challenges successfully. Challenges that are not recognized imply risks. Risks need to be dealt with because they have the nasty habit of sneaking up on you and jeopardizing your success if they are ignored. Recognizing a challenge is usually the first step in successfully dealing with it.

The following discussion makes no claim of completeness—in fact, it is highly likely that you will experience different network management challenges that pertain to your particular context. However, the examples are representative of what to expect and think about.

Technical Challenges

The first and perhaps most obvious set of challenges is of a technical nature. It deals mostly with how to build applications that help with the management of networks and how they communicate with the devices in the networks they help manage. Many of these challenges are familiar to people who have experience in building complex software systems, and many of the same general software-engineering techniques can be applied to help address these challenges. A discussion of general software-engineering techniques is not specific to network management and, therefore, is beyond the scope of this book. However, other aspects are specific to the management domain. Let's take a look at a few of them! Don't worry—by the end of the book, you will have a good sense of how to confront most of these challenges. Later in the book, we dedicate entire chapters to some of those challenges, such as the topic of integration.

Application Characteristics

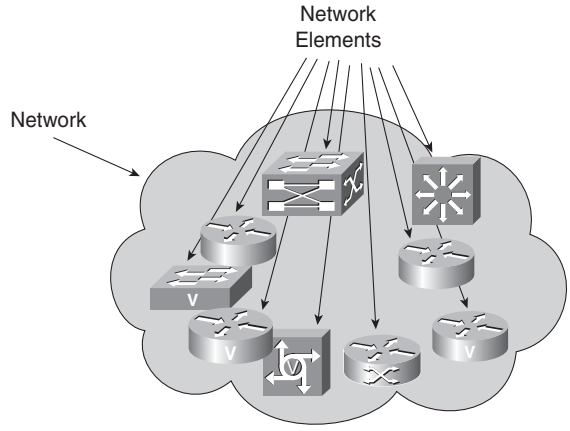
Typically, management systems have to support many different functions. As it turns out, many of those functions really need to be supported through their own (sub)applications. Many of these applications have characteristics with certain architectural implications.

We discuss management applications and tools in greater detail in the next chapter. However, let us preview some typical and important types of network management applications to illustrate the wide range of application characteristics that are involved. Each of them is associated with its own set of challenges. In addition, many of these applications impose different requirements on the supporting management systems, which, from a software engineering point of view, sometimes can be difficult to reconcile. In particular, this concerns characteristics that management applications share with transaction-based systems, interrupt-driven systems, and number-crunching applications.

Transaction-Based System Characteristics

Provisioning applications are concerned with driving desired configurations down to network devices; for example, to turn up a service for a customer in the network. Using network management parlance, we also refer to network devices as network elements, as depicted in Figure 1-8. To perform provisioning, a management system typically sends a request, or a number of requests, to a network element, or a set of network elements, and processes the responses returned from the network to make sure everything is in order. These interactions with the network devices constitute transactions that are conducted with the network.

Figure 1-8 *Network and Network Elements*

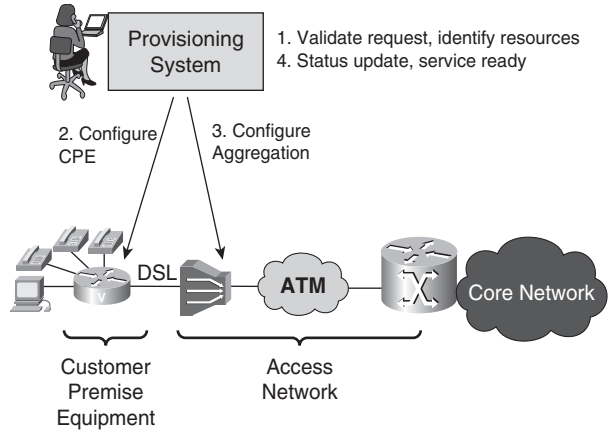


This means that a provisioning application shares many characteristics with transaction-based systems in other areas, such as banking. As with a transaction-based system in those other areas, a provisioning application must be good at dispatching requests, processing responses, managing

jobs, and keeping track of the workflow. (Of course, some differences also exist. For example, unlike in a banking application, the provisioning application needs to deal with devices in a network that in some sense have a life of their own. Changes in the network element's state can occur unexpectedly, outside the control of the operations support infrastructure. Likewise, unlike with bank transactions, some of the operations that are performed might have effects that are potentially impossible to undo, such as when a reset occurs or a line is blocked that causes a glitch in service for some customer.)

Figure 1-9 depicts the role of a management application used for provisioning in simplified fashion. Roughly speaking, the application first confirms that the request for a new service is filled out correctly and identifies which pieces of network equipment are needed to fulfill the request. It then sends a series of configuration commands to the devices that are involved. Finally, it confirms that the newly provisioned service is working. If any errors occur during execution of the transaction, the provisioning application must perform any needed rollback operations to bring the network back to a well-defined state.

Figure 1-9 *Network Provisioning*



Few people would consider a bank transaction system that must serve automatic teller machines in thousands of locations for hundreds of thousands of customers and their associated bank accounts to be trivial. Compare this with a provisioning application that must serve hundreds of operators for tens of thousands of network elements. The numbers for the provisioning application might be an order of magnitude smaller, but consider now that the network elements might comprise dozens of different equipment types and technologies, and support service for hundreds of thousands of customers, each requiring a distinct set of parameters to be configured properly to obtain service.

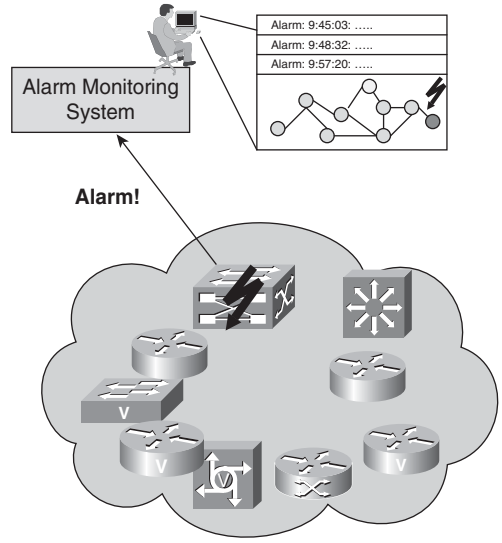
Interrupt-Driven System Characteristics

An important aspect of network management concerns keeping track of the health of the network. In particular, this involves monitoring the network for any alarms that network elements emit. Network elements emit alarms whenever unexpected events occur that might require management attention. In many cases, this involves unusual conditions or failures in the network that require immediate action to avoid degradation of service to customers. With communications services, time is money quite literally—after all, every second of service outage leads to loss of productivity of users in an enterprise and lost revenue to service providers. Alarm monitoring applications can receive and process such alarms, enabling the network manager to get an accurate view of the current state and health of the network, and alerting the network manager to take action when it is required.

Figure 1-10 sketches the function of an alarm monitoring system. Alarms that are received, for example, are displayed on a graphical user interface (GUI) and icons animated with color indicate whether a device is healthy or whether it is currently experiencing problems.

By their nature, alarm monitoring applications call for interrupt-driven systems with real-time or near-real-time characteristics. In a way, they share characteristics with stock-brokering applications that need to keep users updated in real time with constant fluctuations in the prices of thousands of different stocks and alert them of any unusual stock movements because failure to react quickly can result in large amounts of money lost. Again, most people agree that building such a stock-brokering application is not trivial. Compare this with the need to reliably keep network operators up-to-date with the state of thousands or tens of thousands of network devices and service for hundreds of thousands of users.

Figure 1-10 *Alarm Monitoring*



Number-Crunching System Characteristics

Service providers need to analyze networks for their performance for many reasons: to identify bottlenecks, assess whether service levels are being met, evaluate utilization of network resources and efficiency of the network, understand traffic patterns, and analyze trends for planning future network rollout. Generally, this requires collecting and sifting through large volumes of data, including large numbers of data points collected continuously over different periods of time.

The comparison, in this case, is with weather-forecasting systems that need to sift through and analyze large amounts of data as well, collected at periodic intervals from many sensors, to identify weather patterns. Again, by most accounts, building such systems is not trivial. Similarly, network management applications that perform statistical analysis constitute number-crunching applications that must be highly efficient in dealing with large amounts of data and applying complex algorithms for statistical analysis on top of that.

Scale

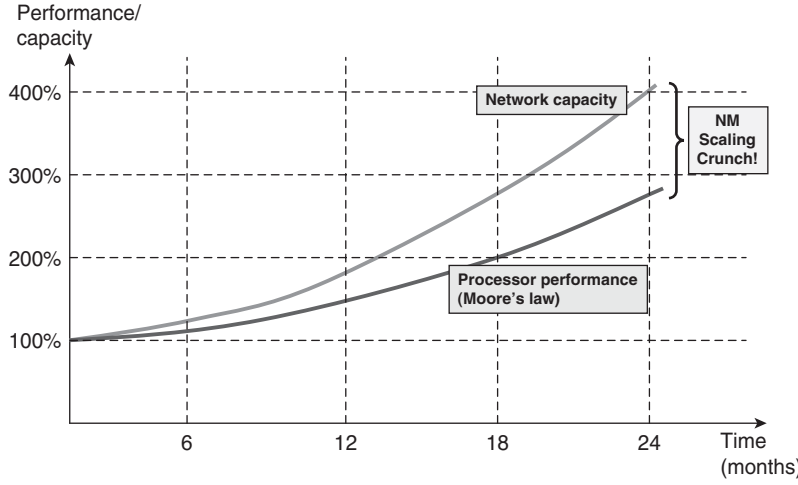
Parents of young children should be able to relate to the following scenario: Try babysitting a toddler for a few hours. When she is hungry, she requires something to eat; you should make sure she drinks enough so she doesn't get dehydrated; perhaps she needs her diaper changed once in a while and a little entertainment to keep her occupied, so you read her a story and offer her some Legos. Doable. Now imagine a toddler birthday, with 20 toddlers and no one there to help you, and things become a little more challenging. While you are changing one child's diaper, another cries that he is hungry, two are fighting over a toy, and you see from the corner of your eye that someone is just about to fall off the sofa and bang his head. Now imagine a football stadium full of toddlers, with you alone in charge. You'll have to start thinking about how to organize things a little differently. The point is, scale matters.

The functionality that a management system provides might not involve rocket science in many cases. However, to be able to build the system so that it doesn't break down as you have to support networks of a very large scale, often much larger than originally anticipated, requires careful architecting and rigorous design discipline. A system that can support a network with a few hundred network elements and a few thousand end users is one thing, but to support tens of thousands of network elements and millions of subscribers, a system might have to be built very differently from the ground up, even if the functionality that the system provides is the same. What it takes to develop a system that can successfully support very large scales is often underestimated. Scale doesn't happen randomly as a byproduct; it must be taken into account at every stage of design and must be specifically architected for.

It must be emphasized that, in general, dealing with scale in applications is a software problem, impacting how the system must be built. It is not a hardware problem, per se. Although it is true that servers are becoming more powerful, relying on increasing hardware performance alone to increase network management system scale is a serious pitfall: For starters, the bottleneck of the

system might not lie in CPU power or even disk I/O. More important, as hardware power doubles, network size and complexity are likely to more than double, making Moore's law of doubling CPU price/performance every 18 to 24 months possibly work *against* network management applications, not for them (see Figure 1-11).

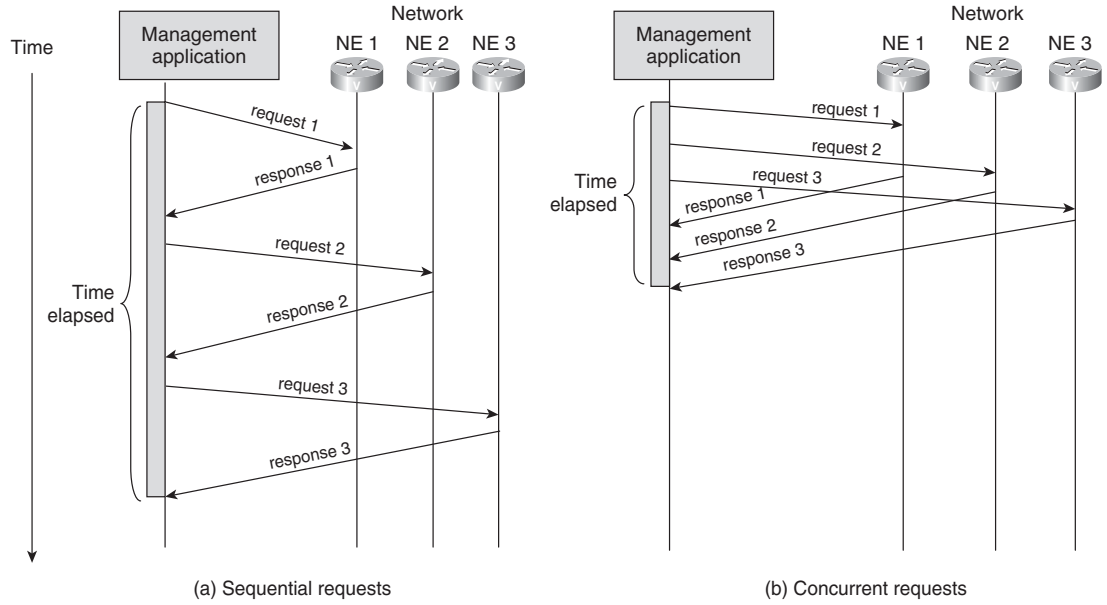
Figure 1-11 *Network Management Scale Crunch and Moore's Law*



The following aspects need to be considered when designing network management applications for scale:

- **Operations concurrency**—How to maximize concurrency in communications to network elements, to maximize management operations throughput. For example, instead of sending a request to a network element, waiting for the response, and then sending the next request to the next network element, it is preferable to send several requests to network elements at once, collecting the responses successively (see Figure 1-12). This way, the management application uses the time of the communication delay productively, and network elements can process requests by management applications concurrently instead of sequentially. As a result, more gets done over the same period of time.

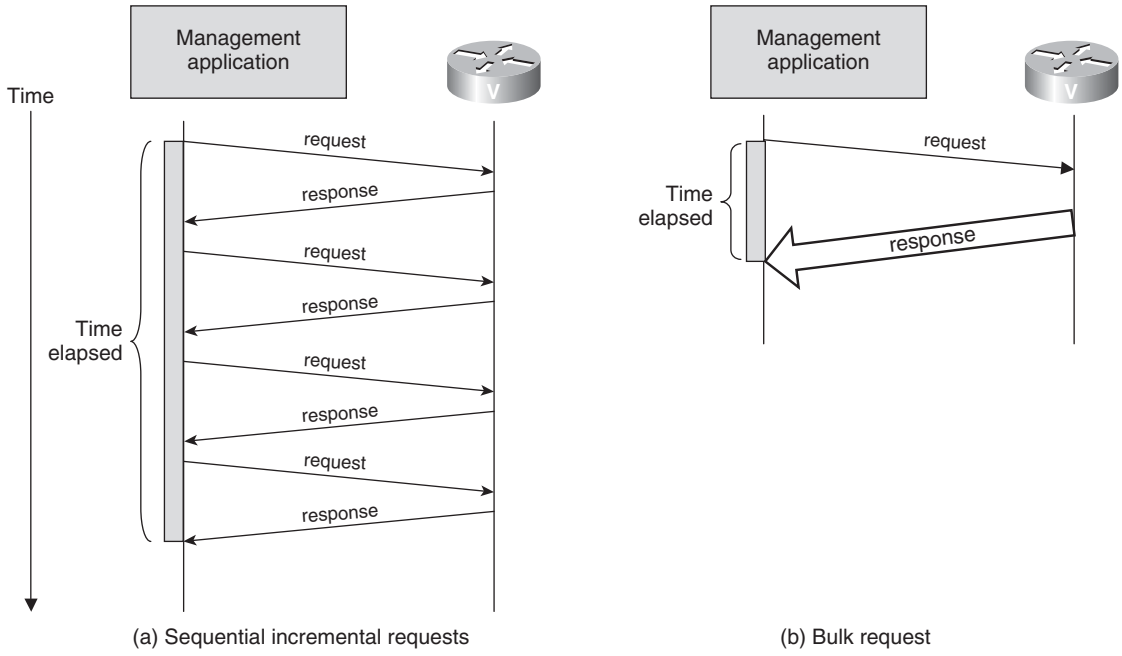
Figure 1-12 *Impact of Operations Concurrency on Operations Throughput*



- **Event propagation**—How to allow events to propagate efficiently to the system and update state. For example, when an event is received from the network, the management application needs to quickly identify where the event belongs (to which device, which card, which port), what its implication is (does the event call for intervention, or can it be ignored?), and what else might be affected (does the event mean that other devices are impacted, are communications interrupted, are customers experiencing a degradation in service?).

- **Scoping**—How to access and manipulate large chunks of management information efficiently and through single operations, without the need for tedious incremental operations (see Figure 1-13). Compare this to the analogy of network management and throwing a party—it scales much better to carry a tray with dishes between kitchen and guests instead of shuttling back and forth to carry every item individually.

Figure 1-13 *Impact of Bulk Operations on Management Efficiency*



- **Distribution and addressing**—How to allow processing to be distributed across different systems to allow the introduction of additional hardware horsepower when required, and how to provide for location transparency and efficient addressing to shield application logic from such distribution. Again using the party analogy, when you unexpectedly go beyond a certain number of guests, you would like to be able to increase your food preparation capacity. If you have only one caterer and one oven, you might be out of luck. To increase your cooking capacity, you would like to be able to add a new oven quickly and thus "distribute" the cooking across several ovens and pots and pans instead of having to upgrade to a larger oven and larger pots and pans, which, beyond a certain size, becomes impractical. Ideally, your caterer will be able to handle increased capacity accordingly. If you had to add a second caterer, it would require you to coordinate between them and keep track of which caterer is responsible for what, which you would rather not do. This means that you want to keep the fact transparent that distribution has even occurred.

One final word concerning how to measure scale: Most network management providers claim that their management applications are scalable. Statements such as "supports millions of objects" are often made. But what does that mean? Do those objects consist of a Boolean true/false flag, or do they represent entire devices in the network? Would they be synchronized with the network resources that they represent up to the minute or once per week? Does the application require a

supercomputer to run on, or will a PC do? Clear metrics, such as those in the list that follows, are required. Of course, to be comparable, claims for scale must all be based on clearly defined hardware configuration and system load:

- Management operations throughput (per time unit, with stated assumptions on the nature of the operations, the number and complexity of parameters, and the number of network elements involved)
- Event throughput (per time unit, maximum throughput [a burst over a short period of time] and sustained, raw receipt of events; or including some kind of processing, again with a predefined scenario)
- Network synchronization capacity (for example, how many network elements an application can synchronize with—that is, retrieve information from—in a given unit of time)

As a side note, it should also be mentioned that, in addition to scale from a technical standpoint, service providers and enterprise IT departments expect a management system to realize economies of scale. This means that the incremental network management cost to introduce more capacity and network elements to the network should get smaller with the size of the deployment. On the flip side, not only large scale, but also small scale can be an issue. For instance, before going to large-scale network deployments, field trials of much smaller scale generally are conducted to verify the soundness of a network solution. For these scenarios, it is important that the cost of the management solution does not become prohibitive.

Cross-Section of Technologies

Building network management systems involves many different technical areas, each requiring its own specific subject matter expertise. Therefore, a firm grasp of a wide array of technologies is required to build effective nontrivial network management systems. This makes network management a technically demanding discipline because it requires a significant amount of breadth in technical expertise.

Let us take a look at some of the technologies that are typically used in network management.

Information Modeling

The centerpiece of any management application is how the application domain is modeled—that is, how network devices, cards, ports, connections, users, services, and dependencies and relationships among them are represented. The resulting models are abstractions of the real world that management algorithms and network managers have to operate on. Ideally, management applications are model driven to a certain extent. This makes them easier to extend and maintain, which is very important, given the constant technical evolution of networks and services that need to be managed.

Successful information modeling requires expertise with object-oriented analysis and design techniques and methodologies, such as the Unified Modeling Language (UML). To avoid reinventing the wheel, it is helpful to be familiar with the many models that industry consortia and standards bodies have previously defined so that they can be leveraged. Perhaps most important are good modeling heuristics and plain common modeling sense. Modeling, like design, is a creative activity. Often there is no objective "right" or "wrong" way to model, but models surely differ in how adequate they are for a particular problem domain, affecting greatly how effective, at what cost, management applications ultimately are. This requires good technical judgment and a good sense for design trade-offs.

Databases

Management systems typically require persistent storage. For instance, they need to store configuration information with which to provision the network and services. Often they also cache information from the network. This way, they avoid needing to query the network element each time someone asks for it, which improves management application performance and scalability. In many cases, management applications also need to store information that augments the information from the network with application-specific data that is not of interest to (and, therefore, not kept in) lower-level systems and network devices, such as customer information.

Of course, management systems generally use and leverage existing database management systems instead of developing their own custom ones. In addition, modern development tools shield applications developers to a certain degree from database intricacies. However, aspects such as performance tuning (disk I/O frequently is a bottleneck) and efficient mapping of information models that are often object oriented into databases that are usually relational (rather than object oriented) still require familiarity with database technology.

Distributed Systems

By definition, management applications are distributed applications because they involve systems that manage and systems that are being managed. In addition to that, to meet requirements for scale as well as requirements for reliability and availability, it is often required to allow the managing system to be distributed itself. For instance, if a server runs out of horsepower to support a network of a given size, it is desirable for additional hosts to be added to increase management capacity. Likewise, reliability and availability requirements often extend from the network to the management systems, requiring a capability to fail over between systems, resulting in graceful degradation instead of a sudden failure of management capabilities. Maintenance requirements might require that individual systems be taken out of service, allowing others to take over their management duties. Similar requirements exist for the support of global management operations that follow the sun, shifting the main management load, for instance, among operations centers in Los Angeles, California; Barcelona, Spain; and Bangalore, India.

None of these requirements can be addressed simply through hardware. For instance, a reliable server does not protect against outage resulting from, say, flooding of the building it is located in or a terrorist attack. Likewise, there is typically a limit to what scale can be addressed simply by using larger servers. Instead, these issues need to be addressed through software. Therefore, many management applications need to be architected as distributed software systems that can distribute and reassign processing load between servers that can be geographically distributed.

Communication Protocols

By definition, management applications communicate with other systems—the network elements they manage, as well as possibly other management applications. At least as far as network elements are involved, this communication occurs using management protocols. Management protocols define the rules by which the systems that are involved in management communicate with each other. The technical properties of those communication mechanisms and their impact need to be well understood because they can have a profound influence on how management applications should be built. For example, is communication reliable, or can pieces of information get lost? How are pieces of information in the device identified and retrieved? What information throughput can be achieved? As with other networking applications, communications trade-offs need to be well understood to arrive at a sound overall system design.

For example, an event-oriented communication paradigm in which the management application can rely on the network element to inform it of any relevant events and changes in the network has an impact on the required complexity of network elements. In this case, network elements have to be capable of storing and retransmitting events in case they cannot be sent at the moment, they are lost, or their receipt not confirmed. This is considerably harder than having the network element merely try to send an event and then allow it to forget about the event, not knowing or caring whether it ever reached its destination. On the other hand, if a management application cannot rely on being automatically informed by network devices when something important happens, it must poll the device whenever it needs information about the network and find out by itself what, if anything, has changed. This results in higher management communications overhead and has implications on the management application's capability to scale—after all, in many cases, nothing will have changed, meaning that much of the communication is wasted.

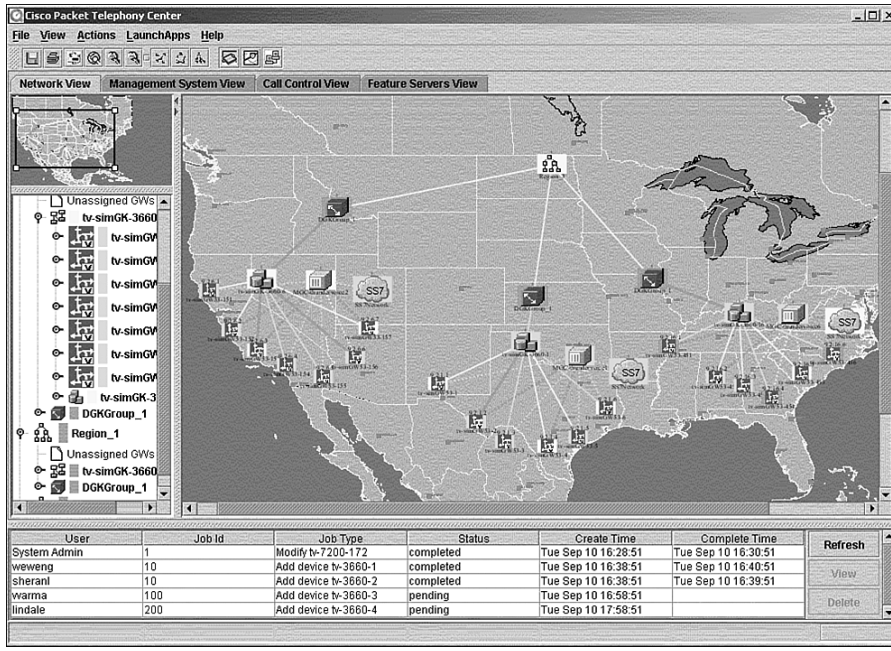
User Interfaces

Last in this list, but not least, human factors need to be considered. Networks can be of enormous scale and complexity. Hence, vast amounts of management information need to be visualized and navigated in an efficient manner. Consideration must be given to how to make operators efficient in performing their tasks: The user interface needs to make the operator productive, as measured, for instance, in terms of the number of operations performed per time unit or the number of network elements that a single operator can safely monitor, while preventing operational errors. In addition to human factors, there is the technical aspect that the user interface back end on a

server must scale well. In many cases, hundreds of operators need to be supported simultaneously, requiring large amounts of information to be exchanged between server and user interface clients, to keep information that is displayed to operators up-to-date.

Figure 1-14 depicts a typical screenshot for a network management application GUI. The network and its topology are depicted on a map, with icons color-coded to immediately give an overview of the overall health of the network. Different ways to navigate the map and zoom into different portions are provided, including a listing of what's in the network that follows a file explorer metaphor. Tabs are used to switch between tasks, and subscreens provide the user with the most recent noteworthy events in the network or the status of management tasks that were recently issued.

Figure 1-14 *A Typical Screenshot of a Network Management Application*



Other Considerations

In addition to the technologies that are required to build a management system, a good understanding of the managed technology itself is required—that is, of the managed network and services. Specifically, an understanding of what aspects are unique about the network and services that need to be managed is required, along with an understanding of what aspects are fairly generic and might be common to other managed technologies. For example, management of a voice network and management of an optical transport network have many aspects in common—for

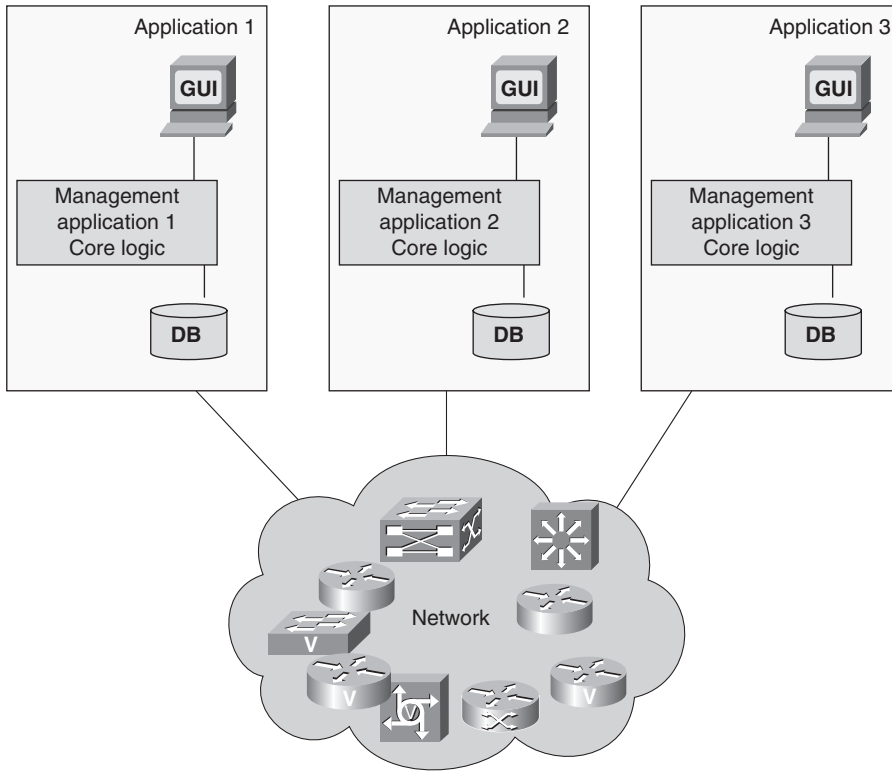
example, topologies need to be displayed on a map, devices must be monitored for alarms, and inventory must be tracked. Other aspects are completely different—for example, the voice network requires management of the dial plan that allows voice calls to be directed to their destination according to the phone number dialed, whereas management of the optical network might involve managing how optical links that carry different wavelengths of light can be cross-connected.

Finally, an understanding and appreciation of the network provider's workflow are required, along with how the management system fits in with the overall operational structure—what the management system is intended for in the first place. A thorough understanding of the system's purpose and how it fits in with the larger context of overall network operations is of tremendous value because it facilitates prioritization between requirements and provides guidance when trade-offs between certain system aspects are required.

Integration

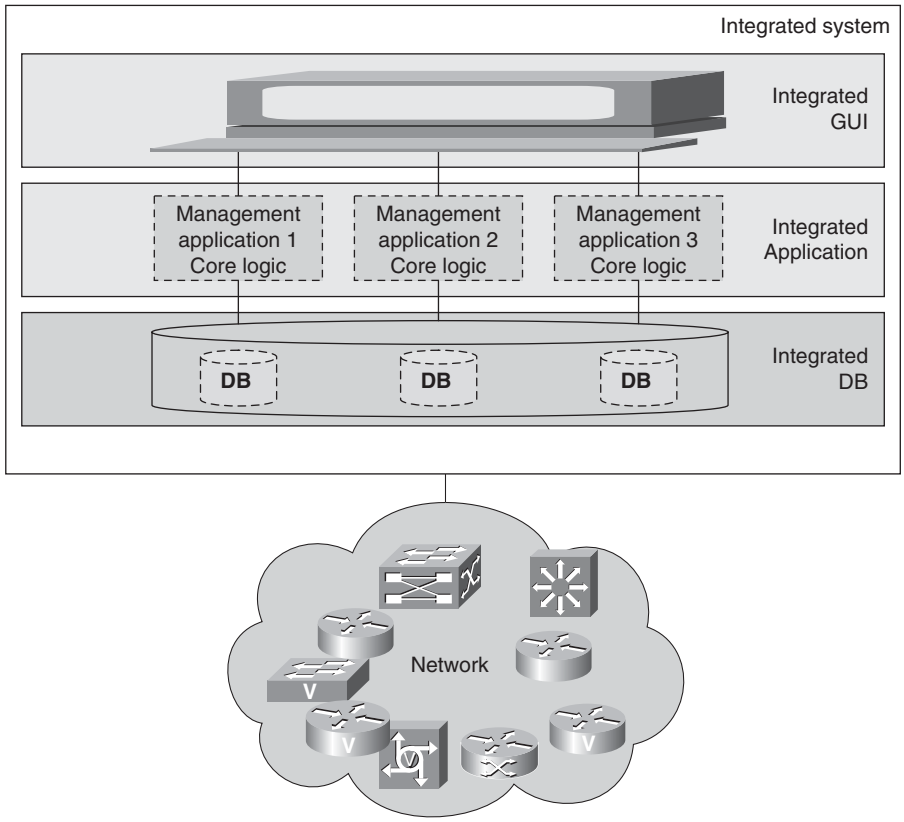
One of the major themes in network management concerns integration. We already hinted at the fact that different applications can be used to monitor a network and to provision services over a network. Likewise, a network probably contains equipment from different vendors, each of which may come with its own set of management software. This leads to an undesirable situation in which the organization running a network must deal with many different applications, as Figure 1-15 depicts. Users need to be trained on all of these applications, and shifting between different tasks might be awkward because the user must switch back and forth between different applications. Often this leads to the so-called swivel-chair syndrome, named after an operator who sits in a swivel chair to move more easily between different terminals, each providing access to a different application. Of course, we don't even want to mention the task of having to administer all the different hosts to support the different applications, each running its own different operating system and database version.

Figure 1-15 *Many Different Applications to Manage a Network*



This situation leads to the demand for integration—that is, the requirement to make all the various applications and systems needed to manage a network work together as if they were one "system"—resulting in a seamlessly integrated operations support infrastructure, as shown in Figure 1-16. Probably one of the biggest complaints that network management providers hear is that the technical solution offered to manage a network is not "integrated" enough. This is a requirement that is very easy to state but that can be very hard to meet; in fact, it is one of the most important reasons why network management can be hard. The need for integration is one reason why standardization is an important topic in network management. Much of the standardization work—for example, standardization of the information that must be exchanged between systems—aims at making integration between different systems easier.

Figure 1-16 *Management Integration—System View*



We do not dive deeper into this topic here. Instead, an entire chapter later in the book is dedicated to this topic (see Chapter 10, "Management Integration: Putting the Pieces Together").

Organization and Operations Challenges

Small networks, such as those deployed by small businesses, might be run by a single person or network administrator as a part-time job. In those cases, how to run the network isn't much of an organizational issue: The network administrator is in charge, and if problems arise that the network administrator cannot solve (or if the network administrator is out sick), customer support by a third party, by the equipment vendor, or by a consultant is only a phone call away. In addition, many communication services such as web hosting or voice services are simply purchased from an outside service provider.

However, running larger networks is different. As outlined in the previous section on technical challenges, scale matters. Also, larger networks might incorporate a much larger variety of different types of equipment and network technologies, making it a lot more difficult to find the combined expertise to deal with running a network all in a single person. Additional dimensions of running the network begin to appear: Help desks have to be introduced. Network technicians need to be dispatched to the field to deploy equipment. Billing disputes need to be resolved.

This indicates that management tools and technology are just one aspect of network management. Running a large network is in many ways an organizational task, truly a management task in the more general sense of the word. Running a network has a lot in common with running any other business and shares many of the same challenges. It is not unlike running a railroad, running a production line, or running a catering business. Although general principles of business administration are outside the scope of this book—this is, after all, a book on network management technology—you should keep in mind that there is an entire other dimension that is an important part of successfully running a large network as well.

In the following section, we point out just a few of the organizational aspects that need to be addressed when running a large network.

Functional Division of Tasks

Question: How do you swallow an elephant? Answer: One little piece at a time. The way to deal with a task of significant complexity is to divide it up into smaller parts. Already the Romans knew *divide et impera.* (Divide and rule.) When you can get your hands around each of the subtasks, you have a good handle on the entire problem. In some cases, of course, the subtasks still need to be divided up further, but you get the idea.

Now there remains only one little detail: *how* to divide the task of running a network. There is no single way to do it, and different organizations find different answers to which way works best for them. However, it is important to keep in mind the different functions that need to be performed and be accounted for. (We dive into this particular aspect in Chapter 5, "Management Functions and Reference Models: Getting Organized.") Identifying what those functions are and organizing around them is a useful first step in identifying a proper division of tasks. An important additional aspect concerns identifying the interdependencies between these functions. The interdependencies determine how different roles and functions need to interact and coordinate, and what interfaces between them are required. Clear interfaces, clear ownership of tasks, and minimization of interdependencies are hallmarks of many successful organizations, and organizations that run networks are no different.

Typical functions and tasks to consider include the following:

- Network planning, for example to determine network topology, dimension nodes and links, and plan for proper network rollout
- Network deployment, to install and commission equipment into the network
- Network operations, to monitor the network for any problems, failures, and issues with performance
- Network maintenance and maintenance planning, to perform equipment and software upgrades, provision services, and tune network parameters
- Workforce management and truck dispatching, to manage maintenance and deployment personnel, which might need to visit remote sites when performing tasks remotely is not possible
- Inventory management, to keep track of what is and what should be in the network, and to maintain spare equipment
- Order management, to take orders for services from customers, dispatch requests to get the services provisioned, and track their execution
- Customer help desk, to provide a front end to customers and provide level 1 support—that is, take calls from customers, answer simpler questions, and, if needed, direct customers to the proper contact for help
- Billing, and billing dispute resolution, to charge customers and collect revenue (very important if you are a service provider because ultimately this pays your bills)

Geographical Distribution

Large networks can be geographically distributed around the globe, along with their users. The network must be managed and users supported globally and around the clock. Often this occurs in follow-the-sun fashion. This means that operational responsibilities get handed off at the end of an 8-hour workday from a network operations center in Europe to a center on the U.S. West Coast, then to Asia, and then back to Europe. The organization itself also must be equipped to handle such rotating responsibilities for different tasks.

Operational Procedures and Contingency Planning

A network provider needs to ensure that the network is managed in an orderly fashion and must stay in control of the functions that keep the network running at all times. To this end, introducing comprehensive and consistent operational procedures and guidelines and documenting is an important tool. This establishes a process that helps ensure that activities can be tracked in an

orderly fashion and that tasks do not fall through the cracks. Examples include ensuring that issues that require responses to customers are not lost and that, for example, equipment configurations are not changed without anyone knowing, which might cause problems later. Documented guidelines ensure a consistent way of dealing with network management tasks and problems, which facilitates a certain level of quality in network operations. Accordingly, these are an important prerequisite to be able to certify quality (think of process quality standards such as the ISO 9000 suite of standards) of network operations.

Part of the operational procedures should deal with contingency planning. What should be done in case of a virus outbreak inside the network or if the network is under a denial-of-service attack? Planning for these types of contingencies and establishing action plans beforehand is an important factor in being able to deal with them successfully and swiftly if they occur.

In a similar way, operational procedures need to be designed to establish a system of checks and balances. For example, authorizations of who is allowed to perform what task need to be carefully managed. This also helps limit vulnerability to sabotage from the inside. Given that people in a network operations organization have access to the network in a way that hackers can only dream about, this is a reasonable consideration in this age of security concerns.

Business Challenges

Technical and organizational network management challenges are there to be conquered. As in most other areas, when the business proposition is sufficiently clear and there is lots of money to be made, the motivation and commitment to overcome those hurdles will become high enough that good solutions eventually follow. However, there are also aspects in the business environment that make network management and, specifically, the development of network management applications, challenging. This is especially the case when application functionality is closely tied to the network equipment instead of, for instance, service management.

Of course, network management encompasses a broad range of functionality. It encompasses management of individual network elements as well as management of business processes surrounding the operations of the enterprise providing network services as a whole. The business proposition for providing management support depends to a large degree on the particular management function. Challenges vary in terms of which aspect of the network management value chain is addressed by a network management application, a targeted market segment, and so on.

In the following subsections, we take a look at some of the more common business challenges. The challenges presented do not constitute a comprehensive list, but they point out some areas that need consideration.

Placing a Value on Network Management

Although network management is vitally important, there is also a flip side: Network management costs money. The amount of investment in network management must be justified, and this ultimately is a business decision. It must be justified by expected cost savings or increased revenues. Ideally, the value proposition must be quantifiable in dollars. Return-on-investment models for network management are needed. Unfortunately, such models can be hard to come by.

In general, service providers expect that no more than a certain fraction of a networking investment should go into network management; as much as 90 percent might go into the equipment itself, and 10 percent into the operations support infrastructure—almost a 10-to-1 ratio. (This includes management of both network and services; the ratio can be even more pronounced for the portion of the infrastructure that manages just the equipment itself.) In many cases, this does not reflect the actual cost structure of network equipment development and management system development, nor the value proposition that network management offers to service providers:

- To an equipment vendor, the development of network management capabilities might cost more than the 10-to-1 ratio indicates. (Of course, unlike equipment, the incremental cost of goods sold is marginal for management software.) This means that, in terms of direct revenue opportunity, it can be more difficult to recoup investment in management application development than investment in networking feature development. Of course, there are other benefits of providing good management support, but they are less tangible and more difficult to measure.

- On the other hand, the operational cost of a service provider might actually exceed the cost for amortization of the equipment. It is often a lot higher than a 10 percent ratio of investment in network management might indicate. This means that limited gains in operational efficiency translate into disproportional gains in terms of overall cost. Statements such as this are not unheard: "As much as 25 percent of the workforce of typical large service providers could be redeployed if it were not for the inefficient operational support provided by the available management solutions." On top of that, in many cases, it is difficult to obtain personnel with the required skills, making the lack of effective management applications a bottleneck to the overall business, thereby implying additional cost from lost opportunity.

So where does the discrepancy come from that leads to a lower business valuation of network management than might be expected? One can speculate about the reason, but some of the discrepancy probably has to do with the fact that it is apparently difficult to quantify the actual value that a management system provides. This is particularly true for many of the "soft" properties of a management system, such as scalability and reliability. Scalability and reliability are the types of properties that can significantly increase technical complexity and, thereby, development cost, as much as an order of magnitude. At the same time, those properties can dramatically drive down a service provider's operational cost. However, unlike with networks in which one might apply measures such as a cost per bit or cost per port, the value of a particular

management system and the properties that it offers are often hard to assess and to prove in a quantifiable manner.

Network providers are thus understandably hesitant to pay a premium. In turn, vendors can find network management investments hard to recuperate and, hence, to justify. This is particularly true for investments in premium features that would have to result in a premium price tag, when in many cases people have difficulty understanding and appreciating even the difference between a simple device viewer and a complex operations support system.

The difficulty of accurately quantifying network management's value proposition can hence lead to significant business challenges. We revisit this topic in Chapter 12.

Feature vs. Product

Traditionally, network equipment vendors have been interested primarily in one thing: selling iron. This is what drives their revenues, profits, and, ultimately, their valuation as a company. Of course, other aspects generate revenue and profits for them, such as services. However, at the end of the day, the success of the vendor comes down to how well the network equipment products do in the marketplace.

Of course, to drive the vendor's business, it is not sufficient to develop world-class network equipment alone. Other aspects have to be offered as well to keep customers satisfied and coming back, such as services, training, and network management. This means that the motivation for network management is, in many cases, not only to make it a self-sustaining business in its own right, but, just as important, to have it serve as a business enabler for the core business. In many cases, it is difficult to sell network equipment by itself. The customer expectation is to get a complete system, which includes network management capabilities offered with it. In that sense, it is easy to view the network management system as a "feature" of the equipment. Of course, network management applications should still generate profit, but this is not the only reason for making a network management–related investment in the first place.

The most tangible business case is still rooted in the revenue contribution made by network management products. However, when viewing network management applications from the perspective of being an enabler of equipment sales, the challenge concerns how to determine the "right" level of investment. Two possible perspectives exist: The first perspective views the development of network management capabilities merely as a cost factor for those other products. Under this perspective, clearly the investment in management applications must be kept to the minimum that is necessary to keep the customer just happy enough to not break the deal. The goal, in that case, is to keep cost as low as possible because additional cost is viewed as simply reducing overall profitability. The business challenge here lies in finding the sweet spot at which investment in network management is just enough to not jeopardize equipment sales.

The second perspective is to recognize network management as a positive competitive differentiator. This changes the business proposition somewhat because development of network management capabilities shifts from being a cost factor to being a revenue enabler. The business challenge in that case lies in being able to articulate the corresponding business case because network management's true business benefit and impact on the bottom line can be intangible and difficult to assess.

Uneven Competitive Landscape

When network equipment vendors offer management applications that are less than perfect, network providers could end up with operational inefficiencies. In general, this should provide an excellent business opportunity for other companies to step in. In most cases, network equipment vendors welcome third-party management vendors who offer network management applications for the equipment vendor's products, and even encourage them to do so: Network management is not the equipment vendor's core product offering, so a competing network management offering is considered less threatening. On the contrary, a third-party offering can help the equipment vendor's customers better leverage their investment and thus buy more equipment. Network providers, on the other hand, gain additional advantages that an independent network management offering might provide, such as support for network equipment from multiple vendors that equipment vendors themselves might not provide. The result can be a win-win situation for everybody.

One business challenge for the management vendor arises from the fact that, in many cases, the equipment vendor will still be pressed to have its own network management offering, for several reasons: to avoid being too dependent on third-party vendors, to avoid having to disclose information on planned products when they are still confidential, or to ensure that a management offering will be available in time when the network equipment is brought to market instead of six months later. As a result, the business proposition for an independent management vendor is often not as attractive as it might otherwise be, for several reasons. Those reasons have to do with the fact that the competitive landscape can be a bit uneven:

- **Timing**—Ideally, a management application should be ready to go to market at the same time as the network equipment that it manages. However, a third-party management vendor tends to lag behind the equipment vendor in offering device support. The equipment vendor often cannot share development plans with an outside company until those plans mature, unlike an internal division developing management applications, which might be cued in from the very beginning. This makes it less likely that the management vendor will be ready when the equipment vendor is ready to deploy. Also, the management vendor might want to wait until it is reasonably sure that the equipment vendor's product will indeed be successful in the marketplace to justify the investment that is required to develop management support for it.

The management vendor cannot afford to chase every lead; it has to use development resources economically, at the risk of coming somewhat late to market. Of course, this means that the first customers of network equipment have to select the equipment vendor's management offering because of a lack of alternatives. As a consequence, they will get accustomed to it even if it has shortcomings and will invest in aspects such as training and even systems integration. By the time a management vendor's product finally goes to market, it might already be too late because network providers will not be willing to switch easily from the system they already have. When an application is deployed in the field, even if it has weaknesses, it becomes very hard to replace it. This results in a high business hurdle for a third-party management vendor to overcome.

- **Economics**—As discussed previously, to the equipment vendor, management software in many cases constitutes a feature of an overall system that also includes the networking equipment. From that perspective, as long as the system as a whole makes a profit, things are fine. The situation is different for a management vendor that considers management software not a part of a larger system, but an independent (and perhaps only) product. The management vendor therefore must generate a profit from the network management application alone to stay in business. Of course, to be competitive, the management vendor's product should provide additional value that sometimes can be more difficult for the equipment vendor to provide, such as support for multiple vendors.

- **Customer expectation**—Customers of network equipment rightfully expect economies of scale. As far as network management is concerned, this means that the incremental cost of management support for the 10,000th network element should be less than the incremental cost for the first. The equipment vendor, on the other hand, will still be able to charge substantially for the 10,000th piece of equipment. Hence, the equipment vendor that views network management as an extended equipment feature can amortize the network management development cost over a substantial volume of networking equipment—a possibility that the third-party management vendor does not enjoy.

All said, the result is a business environment in which it can be fairly hard to make money, particularly when management applications are closely tied to the actual network equipment. This is somewhat paradoxical because management is such an important factor in decreasing cost and increasing revenue, as discussed earlier.

However, the situation is different for management software that is more removed from and less dependent on the network equipment itself. This includes management software that ties together business processes or, for example, billing software. Those are the areas where the playing field shifts more in favor of the management vendor.

Chapter Summary

In this chapter, to set the stage for the remainder of the book, we provided a brief overview of network management. Network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. In other words, network management is about running and monitoring networks. Many analogies can be drawn between network management and other areas where complex systems are monitored or where complex operations are run. We discussed the analogy of monitoring the health of a human body, but we could also have used examples involving monitoring nuclear power plants or airplanes in flight. Likewise, we used the example of running a party as an analogy for running a network but could have used other examples as well, such as running operations at an airline or a factory.

Network management should not be just an afterthought to the network itself. Network management plays a significant role in saving cost, making operation of a network more efficient, and ensuring effective use of resources in the network. It is also vital to service providers in generating revenue—for example, by allowing new services to be rolled out more quickly. In addition, it plays an important role in preventing network outages and, if they occur, keeping their duration to a minimum and limiting their effect.

Different players have an interest in network management for different reasons, and therefore approach it from slightly different angles. There are users of network management, particularly service providers and enterprise IT departments that run networks for a living. Some subtle differences exist in their perspective on network management: For service providers, the focus is on maximizing profits; for enterprise IT departments, it is generally on minimizing cost (of course, while maximizing benefit of network ownership). Then there are providers of network management. Equipment vendors provide network management capabilities to enable and complement their communications equipment business, whereas management vendors build best-of-breed systems for particular management functions that equipment vendors do not address, or that they do not address in the vendor- and technology-neutral fashion required by organizations that run networks. In addition, system integrators provide custom-tailored integration of a multitude of otherwise independent applications and network equipment technologies.

Finally, we provided an overview of important challenges that are often faced in conjunction with network management. Many of those challenges are of a technical nature and relate to the fact that management applications tend to be complex systems with stringent requirements in terms of scale, robustness, extensibility, and maintainability. Other challenges are of an organizational nature, including how to best divide the day-to-day operations of running a network, and of a business nature, involving how to create a business environment in which the development of network management capabilities can flourish. To be sensitized to those challenges is often the first step in dealing with them successfully.

Chapter Review

1. Explain the term *network management* in one sentence.
2. We used a patient in intensive care as one analogy to explain network management. Can you think of areas in network management that this analogy does not capture?
3. Can you think of other areas in which you would expect analogies to network management to apply?
4. Give two examples of how network management can help an enterprise IT department save money.
5. Give two examples of how network management can help a service provider increase revenue.
6. A famous requirement for availability is "five nines." This refers to the requirement that a device or a service must be available 99.999 percent of the time. Assume that you have a device with hardware availability of 99.9995 percent. Now assume that an operational error is made that causes the device to go offline for 5 minutes until the error is corrected. Calculated over a period of a month, how much has the operational error just caused availability to drop?
7. How does the perspective under which network management is approached often differ for an enterprise IT department compared to a service provider?
8. Name at least two factors that can be important to the business success of a third-party management application vendor that potentially has to compete with a network management offering of a network equipment vendor.
9. What does the term *swivel-chair syndrome* refer to, and why is this undesired?
10. Name two or more reasons for network management applications to be approached as distributed systems.