



realtimepublishers.com®

*The Definitive Guide™ To*

# Enterprise Network Configuration and Change Management

**VOYENCE™**

*Don Jones*

---

# Introduction

**By Sean Daily, Series Editor**

Welcome to *The Definitive Guide to Enterprise Network Configuration and Change Management!*

The book you are about to read represents an entirely new modality of book publishing and a major first in the publishing industry. The founding concept behind [Realtimepublishers.com](http://Realtimepublishers.com) is the idea of providing readers with high-quality books about today's most critical IT topics—at no cost to the reader. Although this may sound like a somewhat impossible feat to achieve, it is made possible through the vision and generosity of corporate sponsors such as Voyence, who agree to bear the book's production expenses and host the book on its Web site for the benefit of its Web site visitors.

It should be pointed out that the free nature of these books does not in any way diminish their quality. Without reservation, I can tell you that this book is the equivalent of any similar printed book you might find at your local bookstore (with the notable exception that it won't cost you \$30 to \$80). In addition to the free nature of the books, this publishing model provides other significant benefits. For example, the electronic nature of this eBook makes events such as chapter updates and additions, or the release of a new edition of the book possible to achieve in a far shorter timeframe than is possible with printed books. Because we publish our titles in “real-time”—that is, as chapters are written or revised by the author—you benefit from receiving the information immediately rather than having to wait months or years to receive a complete product.

Finally, I'd like to note that although it is true that the sponsor's Web site is the exclusive online location of the book, this book is by no means a paid advertisement. Realtimepublishers is an independent publishing company and maintains, by written agreement with the sponsor, 100% editorial control over the content of our titles. However, by hosting this information, Voyence has set itself apart from its competitors by providing real value to its customers and transforming its site into a true technical resource library—not just a place to learn about its company and products. It is my opinion that this system of content delivery is not only of immeasurable value to readers, but represents the future of book publishing.

As series editor, it is my *raison d'être* to locate and work only with the industry's leading authors and editors, and publish books that help IT personnel, IT managers, and users to do their everyday jobs. To that end, I encourage and welcome your feedback on this or any other book in the Realtimepublishers.com series. If you would like to submit a comment, question, or suggestion, please do so by sending an email to [feedback@realtimepublishers.com](mailto:feedback@realtimepublishers.com), leaving feedback on our Web site at [www.realtimepublishers.com](http://www.realtimepublishers.com), or calling us at (707) 539-5280.

Thanks for reading, and enjoy!

Sean Daily

Series Editor



## Foreword

By Glenn O'Donnell, Program Director, META Group

December 2003

Configuration management is a subject that has long been recognized within the IT industry. Indeed, we have been performing this process since the dawn of technology itself, as every action we take to modify the characteristics of the environment is a configuration exercise. The overwhelming majority of configuration tasks have historically been manual. For years, this was not only acceptable, but necessary. It is no longer a viable approach, however, for controlling the scale and complexity of today's infrastructure. Unfortunately, our field still clings to manual task execution despite technology developments toward automation. This is about to change dramatically.

Economic forces bolstered by the aftershocks of the dot-com bubble collapse have irreversibly altered our industry. Today's focus on information technology has shifted from the technology itself to the quantifiable benefits IT can demonstrate for a company's core business. Disciplined operational processes are the essential key to drive IT organizations toward this ideal of business relevance. Most IT organizations require sweeping changes to their operational processes to remain viable. The alternative is dismal, so the incentive is in place to either adapt or wither.

Operational process best practices identify configuration and change management as the center of every basic function within IT. These two principal processes are inextricably linked because all changes to the configuration must follow a structured change process. Emerging active configuration products are therefore merging the two processes under a common technology solution umbrella. Legacy configuration tools often lacked the audit trail or checks and balances needed to follow proper change-management process steps. They also took a device-centric perspective to configuration (for example, change an attribute of all routers, one router at a time). This is certainly an improvement over manual configuration, but requirements have progressed to broader end-to-end services which are outside the capabilities of most products. Next-generation change and configuration management solutions are now addressing more comprehensive service perspectives while offering enhanced process automation and heterogeneous infrastructure support.

The need for change and configuration progress is dire across all IT domains, but the networking space is particularly distressing. Continued manual execution is exacerbated by reliance on an elite oligopoly of experts. These experts are valuable for directing the future evolution of the network and network-based services, but their prominent role in operations is a waste of their talents and, accordingly, a waste of money. Senior IT and business executives understand this issue and express a fervent desire to reduce operational costs while preserving technical leadership for future growth. Prospects are optimistic for all parties, as stronger process adherence and more effective automation tools are within reach. IT organizations that embark on this path to higher maturity will enhance their business value by providing cost-effective services that are reliable and perform well. Doing so will ensure a prosperous future as a valued business asset.

Contact the META Group at <http://www.metagroup.com> or 203-973-6700.

Introduction.....	i
Foreword.....	ii
Chapter 1: Introduction to Network Configuration and Change Management.....	1
What is Change Management? .....	1
A Process .....	2
A Tool.....	3
Why Bother with Change Management?.....	4
Excuses for a Lack of Change Management.....	4
The Operational Risks.....	5
The Financial Risks.....	6
Building a Process.....	10
Where Do You Start?.....	10
The Players.....	11
Tools and Technologies .....	13
Industry Best Practices.....	13
What Else Do You Need to Know? .....	16
Network Change Management and Stability .....	16
Network Change Management and Security .....	16
The Scope of Change Management .....	17
Network Change-Management Technologies.....	17
Network Change-Management Tools .....	18
Network Change-Management Best Practices.....	18
Sample Change-Management Processes.....	19
Summary .....	20

## Copyright Statement

© 2003 Realtimedpublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimedpublishers.com, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimedpublishers.com, Inc or its web site sponsors. In no event shall Realtimedpublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimedpublishers.com, please contact us via e-mail at [info@realtimedpublishers.com](mailto:info@realtimedpublishers.com).

## Chapter 1: Introduction to Network Configuration and Change Management

How does your company handle change management in the network? Do you worry about it at all? My own experience is that 90% of small- to medium-sized companies—those with fewer than about 8000 IT users—rarely practice any serious change management when making changes to their network configurations. I used to work for one of the East coast’s larger network integration firms, who handled outsourced network operations for some of the region’s largest companies. They didn’t do any change management, either, beyond keeping some informal Post-It notes of what changes they planned to make. Don’t be embarrassed if your organization doesn’t practice change management, either; you’re in good company.

But businesses are getting smarter. Today’s ethos of “do more with less” doesn’t allow critical IT resources to become unavailable through a simple manual configuration error. The idea that network management—in some companies, at least—is about as rigorous and scientific as a séance is starting to scare top executives, and they’re asking their network managers to do something about it. That *something* is *change management*, a set of processes and tools designed to ensure that network configuration changes never take the network down, and that provide rapid recovery in the event that they do.

In this chapter, I’ll introduce change management as a concept, discuss the very real business reasons for having it, and provide an overview of how you can begin adopting solid change management practices into your environment.

### Assumptions About Who You Are


If you’re reading this book, then I’m assuming you have an interest in how change management can affect and improve your network operations and stability. You might be a network manager or CIO, or perhaps a senior network administrator.

You might work entirely within your company, meaning that your company handles its own network management all internally. You might also work for a company that outsources all or a portion of its network management to an outside network integration firm. Or, you might work for that outside network integration firm, designing and managing networks for multiple customers.

This book is for all of you. While I’ll usually start a discussion focused on the strictly-internal IT staff, where appropriate I’ll expand the discussion to include outsourcing scenarios, which I’ll cover both from the client and consultant/integrator viewpoints.

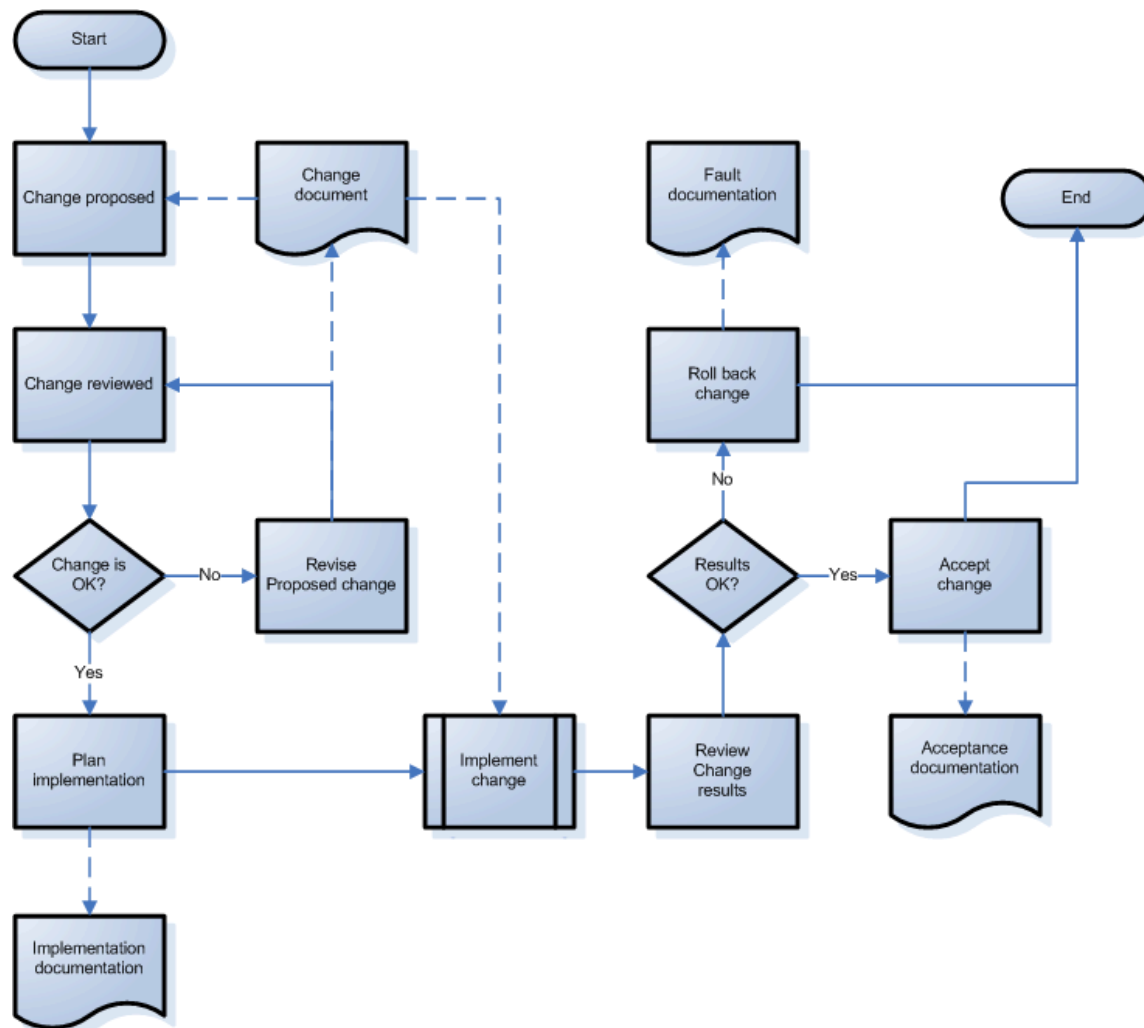
### What is Change Management?

What exactly is *change management*? Browsing around the Internet doesn’t provide much in the way of solid definitions. Is it a set of products you buy? A process you follow? A group of technologies, or a management buzzword? Change management can be all of those things, actually.


 If you want to be picky, *change management* is defined by Dictionary.com as “A set of techniques that aid in evolution, composition and policy management of the design and implementation of an object or system.”

## A Process

At its heart, change management is a state of mind, a philosophy that says “we want to only make changes after due planning and consideration, and we want those changes to be made in a consistent, repeatable, reliable fashion.” Implementing that philosophy usually results in a process, outlining how change occurs. Figure 1.1 shows a simple change management process that might serve as the basis for managing change to networks, software applications, building a house, or almost anything else.




**Figure 1.1: Simple change management process.**

 Later in this chapter I'll present a slightly more detailed change management process; what's important to remember is that every organization will come up with something slightly different that best suits their needs and their environment. In developing your own process, plan to borrow from others to create your own unique solution.

All change management processes usually involve some common steps:

- Formal documentation of the proposed change.
- Collaborative review of the change to assess risks and ensure accuracy. This should include testing of the changes in a lab environment to assess their accuracy, as well.
- Timeline for implementing the change.
- Acceptance of the overall plan by stakeholders.
- Final documentation of the change as it will be implemented.

 I'll cover these steps in more detail in Chapter 2. I'll provide sample change-management processes, with explanations of how they work, in Chapter 8.

The process is intended to serve as a set of rules and reminders for how change is reviewed and implemented. Of course, you can't underestimate the penchant for people to work around rules and processes, especially harried network administrators who just want to put out today's fire. Discipline is required to make any process work, and it's also incumbent on the process itself not to present unnecessary hurdles. For example, a network change management process should offer a streamlined way for emergency changes to be implemented. For example, if you find out on Tuesday that your primary ISP will be going offline on Wednesday, then you'll want to quickly make some changes to route traffic through another connection. That's not something you can afford to spend weeks arguing about; your change management process has to provide a way for high-priority changes to be safely and quickly handled.

### **A Tool**

Change management can often be enforced and automated through tools. These tools may provide a variety of functions, including:

- Tracking requests for changes and documenting the details of proposed changes.
- Comparing proposed changes to known-good templates, to help weed out improper changes. Tools may also allow changes to be proposed through a template, ensuring a level of consistency for all submitted proposals.
- Enforcing a workflow process that requires peer or supervisory signoff.
- Basic boundary-checking to ensure that company policies and security practices won't be violated by the change (such as a change resetting all router admin accounts to have a blank password).
- Displaying the exact changes which will be made to devices' configuration files.
- Tracking the change and deploying it to the affected devices.
- Monitoring devices for changes, pulling the changes, and documenting them for review.
- Automatically redeploying a last-known-good configuration to devices which have been changed without authorization.

The variety and capability of change management tools provides a lot of functionality to help businesses better manage their networks.



### Change Management with Vendor-Specific Tools

Vendor-specific tools, such as Cisco's CiscoWorks package are well written and provide useful functionality; however, I have yet to encounter an environment that is truly standardized on one vendor for infrastructure devices; there is always an odd device out: a firewall, load-balancing device, switch, and so on. In fact, most companies with perimeter networks (or demilitarized zones, as they're called) often select firewalls from different manufacturers to provide an extra layer of security. The necessary myriad vendor-specific change-management solutions required for such environments defeats the point of change management entirely; you'll spend too much time in too many different tools to effectively manage change.

Fortunately, there are plenty of vendor-neutral tools that provide support for devices from several manufacturers. These tools offer the advantage of a single user interface (which is often less complicated than the devices' command-line or graphical interfaces), integrated functionality, and enterprise-wide management capability.

The best of these tools have a modular or scriptable architecture, meaning they can support a wide variety of devices and are easily extended to support additional devices in the future—often without requiring the installation of an updated release of the tool. If your organization regularly adopts new technologies, make easy extensibility part of your tool selection criteria.

## Why Bother with Change Management?

A recent industry-wide survey of network managers revealed that half of those surveyed had experienced unauthorized changes to their network. Half of those surveyed also attributed human error—manual configuration changes—to at least 50 percent of their non-carrier related outages (those caused by a downed T1, for example). Those are frightening statistics, and they reflect a very real-world situation: few organizations bother incorporating a formal change-management process into their network management.

### *Excuses for a Lack of Change Management*

In my consulting practice, I hear many reasons that companies give for not having a solid change-management process in place. Some of them are pretty funny:

- We don't have the money. Of course you do! Change management doesn't mean you must buy a suite of expensive tools, although there are some tools that make it easier. Change management can be as simple as flowcharts and notebooks used to track changes and maintain a valid process.
- We don't have time to train staff in change-management techniques. Good change-management process and the right tools can actually *reduce* the need for training. Many change-management tools replace the vendor-specific command-line interfaces and graphical tools, creating a single point of management that requires less training. In addition, many tools offer template capabilities so that junior administrators can manage the network by filling in blanks on a form and selecting valid values from list boxes. If you don't have time to train, change management can offer a solution, not a hurdle!
- It won't happen to us. This excuse barely deserves comment. I have yet to meet a network manager who can actually say this with a straight face. And if a change-related outage hasn't happened to you yet—it will, eventually.

- Our network is too simple. This excuse could be a valid reason not to practice change management—if you define *too simple* as *contains no manageable network devices*. Plenty of small companies get by with a hub or two, so there is no room for error. But you need look only as far as your Internet connection to find a potential failure point, which means you need to make sure that your ISP practices change management (or you could be without that Internet connection).
- We've always done it this way. Will you keep doing it that way forever, even as your business grows more complex and your network grows more complex in response? Try doing things a new way and see how many of your day-to-day problems are a result of the old way. Adopting a solid change-management process may introduce efficiencies you didn't know were possible.
- Our people know what they're doing. Even the most well-trained network administrators will move on eventually, and you don't want them to leave with all of your network secrets locked up in their heads. A solid change-management process, along with the right tools, can make network administrators' jobs easier, give them more reason to stay with the company, and, most important, provide a lasting document of your network so that it truly belongs to the business, not a single individual or group of individuals.
- We don't have time. Implementing a change-management process can be time consuming. One company I worked with spent nearly a week developing their process and probably spent time over the next 2 months refining it. However, in their first full year of using their new process, they had zero network downtime resulting from manual configuration errors—down from 20 hours the previous year. They estimated that those 20 hours had cost them about \$60 million (they process credit card authorizations over the Internet). The time they spent coming up with the new change-management process probably cost them \$20,000 or so in salaries. The bottom line is that you'll pay now or you'll pay later, and if you pay later—when the network is down—it will cost a lot more.

I could go on and on, and I'm sure you've heard unique and interesting excuses in your own organization. Think of it this way: change management for network configuration is like a seatbelt. It takes a few extra seconds to use, and adds a few dollars to the price of the car. Most of the time, you never need it. But that one time you do need it, you're *really* glad you were wearing it. Any excuse not to use it is just that—an excuse.

### **The Operational Risks**


The obvious risk of not having change management is that an ad-hoc change will take all, or a portion of, the network offline. Actually, that's probably the best-case scenario that businesses face if they insist on allowing unmanaged change to their environment. One wrong change could also result in everything from lost data to employee accidents. And then, of course, there's the simple financial risk. How much revenue would your company lose if the network failed for a single hour?

## The Financial Risks

So you make a change and the network goes down. What's the big deal? In real dollars and cents, it's a *very* big deal for many companies. Businesses rely more and more on the 24 × 7 availability of their networks and have very little tolerance for downtime—particularly from a revenue standpoint.

Consider a major ISP such as America Online (AOL) or Earthlink. If they made a change to a network router that interrupted service for all of their users, it might be a day before they figured out what the problem was. But suppose they were only offline for an hour. AOL has millions of users, each of whom pays about \$25 per month for their service, which breaks down to about \$.034 per hour. If only 2 million users—a fraction of their user base—were affected by the change, they could demand refunds, and AOL could be looking at almost \$70,000 per hour of lost revenue.

Online sales of airline tickets are heavily network-dependent and can cost \$90,000 or more per hour in lost revenue, because travelers can easily buy tickets from another source. Home shopping is estimated to bring a company nearly \$114,000 per hour in sales—and that's not even during the busy holiday season. Consider the cost of a network outage to companies that deal in truly large financial transactions: credit card processing firms use their networks to process so many transactions an hour that a single hour of network downtime can result in a loss of \$3.4 million in transaction fees. Online stock brokerage firms—whose very existence depends upon their network infrastructure—can lose upwards of \$7 million *an hour* if the network goes down—not to mention potential lawsuits from investors who lose money because they're unable to access their portfolios or complete an online transaction. If the outage lasted for an entire trading day, the brokerage could lose upwards of \$60 million dollars (and face severe government fines and penalties)—a number that could easily be higher than some firms' entire yearly operating budgets.

 These numbers are my estimates based on sources such as the National Retailers' Association, company earnings reports, and other public sources. IT consulting firms such as the META Group (<http://www.metagroup.com>) also provide reports that include downtime statistics. You can also try a Google search on "network downtime cost" to see various industries' statistics on the subject. The cost of downtime is becoming increasingly important as companies try to do more with less and as they rely more on technology to provide competitive and financial advantages.

One junior network administrator earning \$50,000 a year can put a period in the wrong place in a routing table and cost his company millions of dollars per hour in lost revenue. If you were to tell any CEO or CFO that losing electrical power would cost them that much, they'd have backup generators installed the next day—and many companies that are highly dependent on their network infrastructure do, in fact, have battery backups and backup generators. Yet those same companies muddle along with manual configuration processes that involve little or no change control, essentially gambling that nothing will go wrong.

How much would your company lose in a day? In most companies, you can assume that a network failure will create a pretty severe impact, but you'll need to look at how dependent your company is on the network. If all the computers were shut off, how long could your company continue doing business without email, the Web, Word, or Excel? If you're using an IP telephony system, you might not even have telephone service.

Obviously, *any* amount of revenue lost to a simple network configuration mistake is unacceptable, particularly when the right process and the right tools can prevent the mistake entirely. Thus, you need a process to make sure it doesn't happen.

### The Case for Change Management

One of my customers provides an excellent example of the benefits of change management. They are a large bank that handles credit cards, authorizations, and loans, providing these services to other banks that are too small to maintain their own operations. The company is centrally located in a fairly large campus that houses about 20,000 users. All of the company's desktop computers are handled by one group, while the network infrastructure is handled by another. This interesting division of labor is common and from a statistical viewpoint is a goldmine: The various IT groups treat one another as outsourced agencies, and they perform a lot of tracking on the work they do. For example, company policy allows no more than 200 devices or computers per IP subnet, reserving the 50-odd remaining IP addresses in the subnet for supporting devices and emergency growth. So when the desktop support folks are setting up a new call center, they place a request with the infrastructure team to create a new subnet and add the appropriate routes to the network's routers.

The infrastructure group categorizes requests into two basic groups: emergency and planned. An emergency request is just that—something has gone wrong and needs to be fixed. A planned request is a task—such as adding a new subnet—that needs to be done on schedule but not immediately. When I first started working with the company, they didn't have any change-management processes in place. As Figure 1.2 shows, the average response time for an emergency request was about 3 hours; a planned request was usually handled in less than a third of that time.

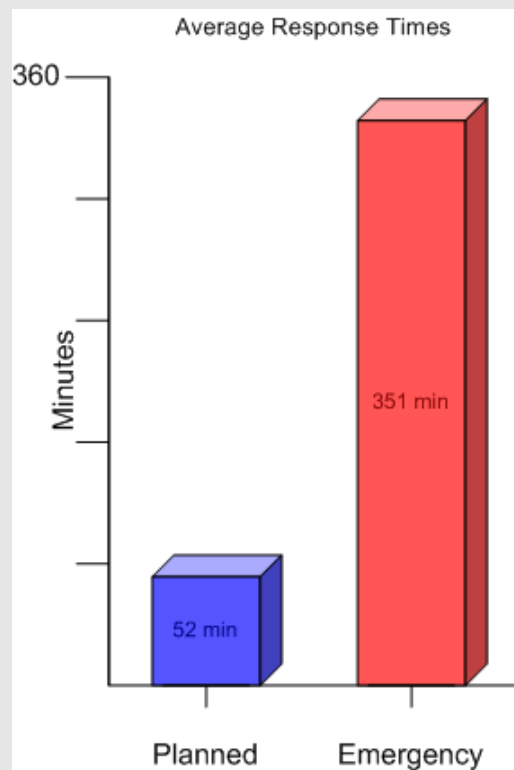
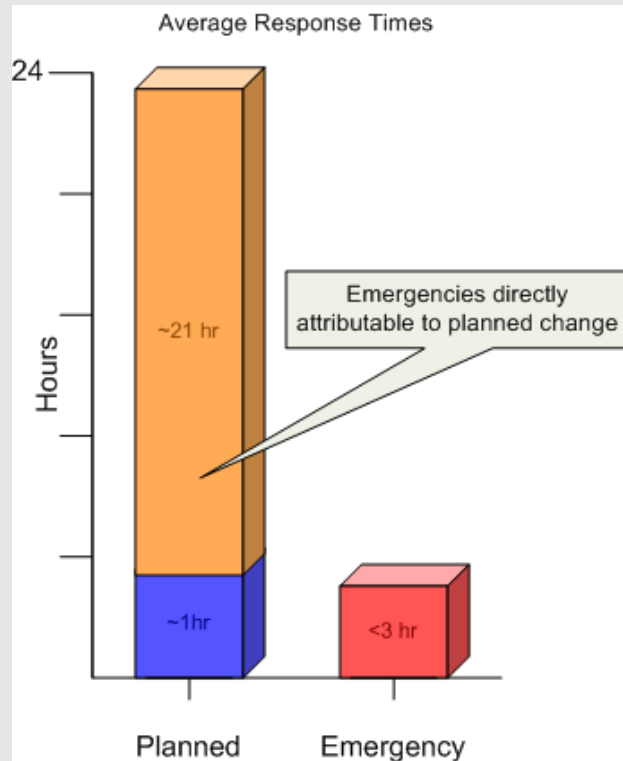


Figure 1.2: Response times for various requests.

When I first started making the case for a change-management process (the infrastructure folks jokingly referred to me as the “change-management police” whenever I showed up), the team’s argument was that they were handling changes just fine—it was the emergencies that were the problem, and change management wouldn’t solve that. So I did some digging in their request tracking system and found that most emergency requests came in immediately after a planned request had been marked as complete. Generally, the documented resolution for the emergency requests involved changing something that had just been done in resolving the planned request.

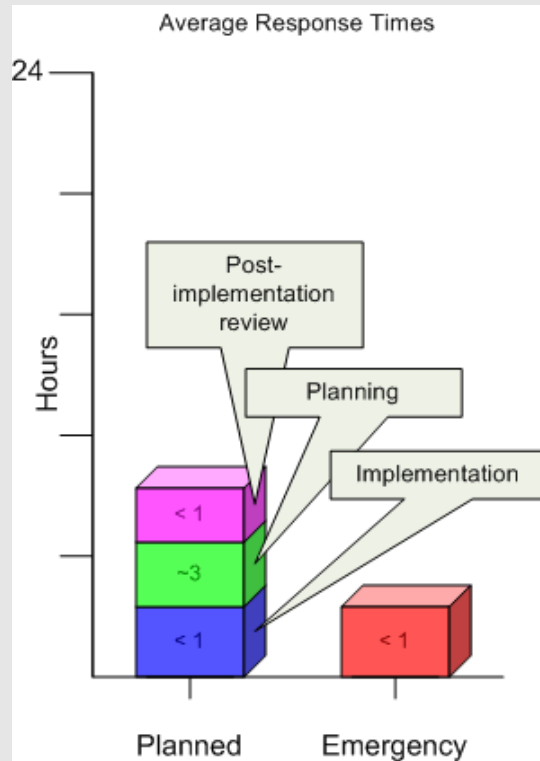
So I redid their statistics. This time, I listed the time to complete the planned request along with the time it took to fix all the things the planned request broke. I listed the true emergency requests—things that couldn’t have been predicted or avoided—individually. As Figure 1.3 shows, the picture was drastically different.



**Figure 1.3: Response times more appropriately grouped.**

My contention was that proper change management would have eliminated the hard-to-fix emergencies because the so-called “planned changes” were obviously being implemented ad-hoc and without a lot of care.

The infrastructure group now tracks their time more carefully. The response time for a planned change includes all the time it takes to work through the change-management process as well as the time to actually implement the change (which is usually negligible because that deployment is now automated). Any subsequent emergency that is caused by a planned change is documented as such. Such emergencies are actually rarer now, although they do still occur; after all, the folks handling the change-management process and change reviews are still human. Figure 1.4 shows their new average times.



**Figure 1.4: New response times under change management.**

Notice that the emergency response time is barely even on the chart? The reason is that the group bought change-archival and rollback tools. Even when an entire router dies, they can get a spare unit in place quickly, and use their tools to blast the last-known-good configuration to the spare in just a few minutes. It is tough to work out exactly how much money they're saving, but one recent failure of a core router kept the company offline for about an hour, and management estimates that they lost about \$2 million in revenue. The router experienced some kind of burp and dumped its memory, taking pretty much the entire network offline. The team had to recycle the router, swap one of the cards, and reload the router using their configuration change-management tools. Without those tools and processes in place, the group manager guessed they would have been down for about 4 to 6 hours while a backup was located and loaded into the router. The difference between \$2 million versus \$8 to \$12 million in losses makes a clear case for the fact that change management pays for itself in the end.

## Building a Process

I'll assume that you're on board with the idea of change management in the enterprise at this point and that you're ready to begin developing a change-management process. In the next few sections, I'll walk you through the basic steps and provide an outline for much of the rest of this guide.

### Where Do You Start?

Do *not* under any circumstances start searching the Web for change-management tools. In the IT industry, we tend to look for complete, packaged solutions first, without actually thinking about what we want those solutions to do. Instead of surfing, start thinking about the process you want to build. What should it look like? Who will participate? Which steps will be included? Once you've ironed out the process, you can start looking for products that will allow you to implement that process.

Start by examining the way you currently handle changes. You don't need to make this step a complicated business-process analysis; just grab a pen and a piece of paper and sketch out what really happens in your existing environment. Something rough and simple, like the flowchart that Figure 1.5 shows, will do the job.

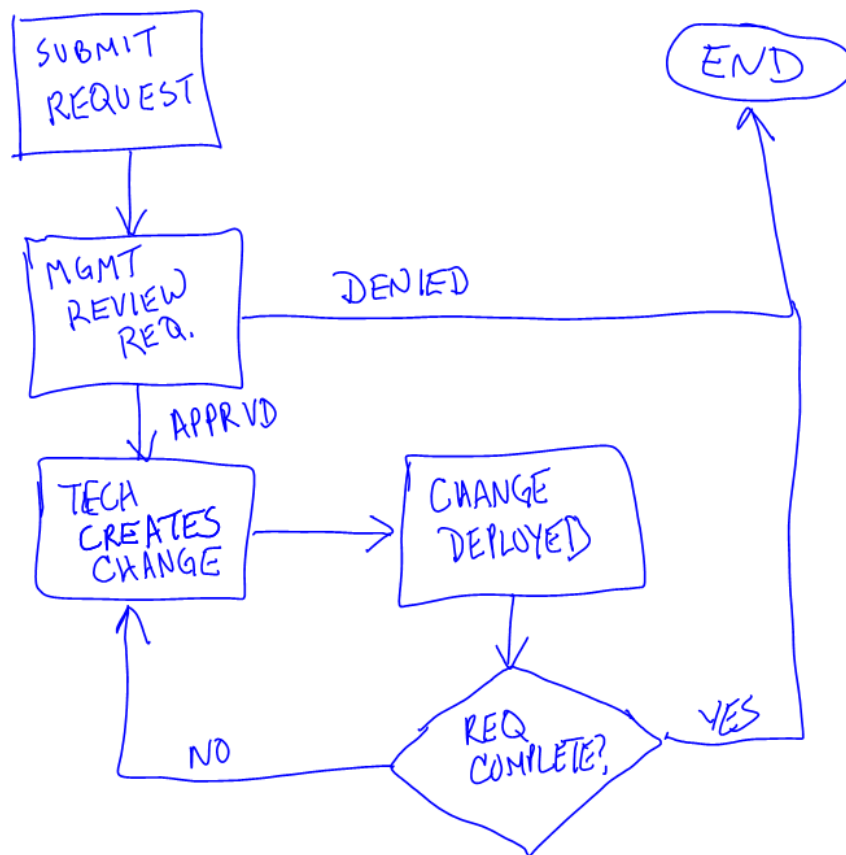


Figure 1.5: Understanding your existing process.

Now you have something to start with and you can begin to identify areas where things will go wrong. For example, ask yourself whether the existing process incorporates the practices you think are needed. Using the process in Figure 1.5 as an example, here are some obvious weak points:

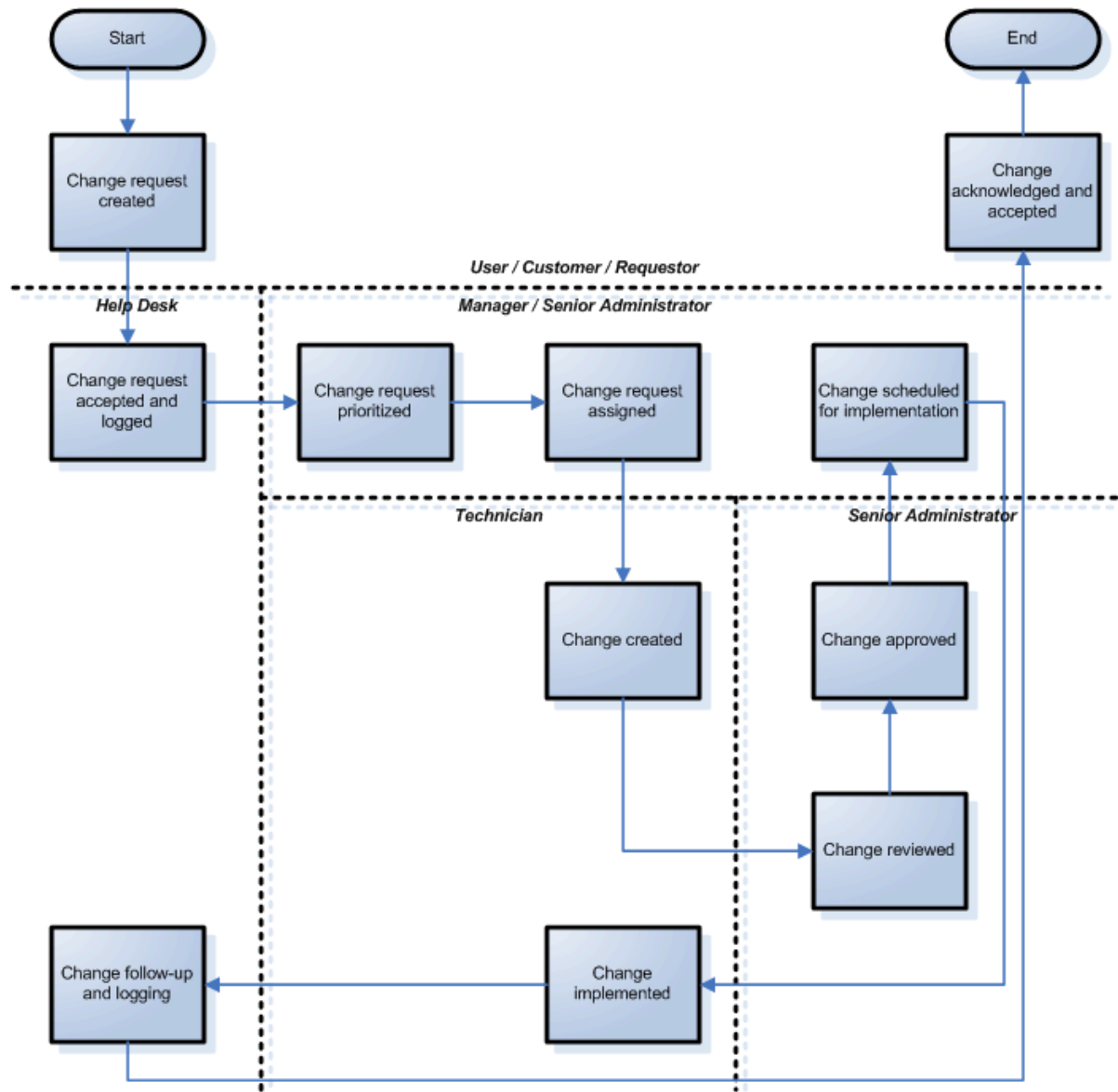
- The change isn't documented.
- There is no peer review of changes before they are implemented.
- Management has no input into the schedule of change implementation, meaning implementation may be unexpected or poorly communicated.
- Technicians can engage in an iterative process of changes until they feel they've completed the request; this process can lead to additional unnecessary downtime.
- Changes aren't archived and there isn't a process for rolling back changes that don't work out the way they are supposed to.
- Changes aren't prioritized or categorized, meaning that even important, urgent changes may be treated as longer-term changes.
- This process makes it seem as if network technicians keep most of their "documentation" in their heads rather than on paper or in a file where others can access it.

In addition to these weak points, there are several missing elements—you can probably spot additional things that you would like to see added, so do so. Pull out more paper or even an application such as Microsoft Visio, and start developing a process that meets your needs. As you go, make notations about where tools might be able to help. For example, if you add a step to "archive existing configuration" that happens before any changes are made, you might make a note to look for tools that can automatically archive your device configurations. For a "deploy change" step, you might look for tools that can automatically deploy changes consistently to multiple devices or even do so after hours when fewer users will be impacted. To enforce constancy, you might look for a tool that provides engineering templates.

### ***The Players***

You need to get an understanding of who is involved in your change-management process. One way to do so is to sketch out your current or proposed process in broad terms, including only primary tasks and not a lot of detail. Draw dotted lines to separate roles, and name those roles. For example, Figure 1.6 shows a process flowchart that includes requestors, management, senior network administrators, technicians, and a requestor point-of-contact in the form of a Help desk.





**Figure 1.6: Understanding the players in your change-management process.**

Although this type of flowchart might not be the most useful when it comes to ensuring a safe and reliable process, it can highlight unnecessary redundancies and bureaucracy in your project, giving you an opportunity to streamline the process if desired. For example, in the process that Figure 1.6 shows, the manager might include a tentative schedule with the request assignment. That way, when the peer review by the senior administrator is complete, the process could flow immediately back to the technician for implementation because the schedule has already been set. An exception flow could be provided for changes that take too long to review and fix, making the scheduled no longer feasible; such a revision would provide a more streamlined process for the majority of changes, while providing support for changes that can't be accommodated within the streamlining.

## Tools and Technologies

Now—with your process behind you and all the players identified—you can begin evaluating tools and technologies to help with your change management. Tools should *never, ever, ever* be a driving force behind how your process is built. In fact, if you're looking at change-management tools that enforce a particular process, stop looking at them. Good tools should fit *your* model, not their manufacturers'. In fact, good tool vendors will tend to start out a sales discussion by asking you what your process looks like.

One of the things I'll cover in subsequent chapters is how to develop an evaluation process for change-management tools. I'll highlight important features and describe how they can be useful, then show you how to conduct an evaluation of multiple products to select one that contains the features that are most important to your organization.

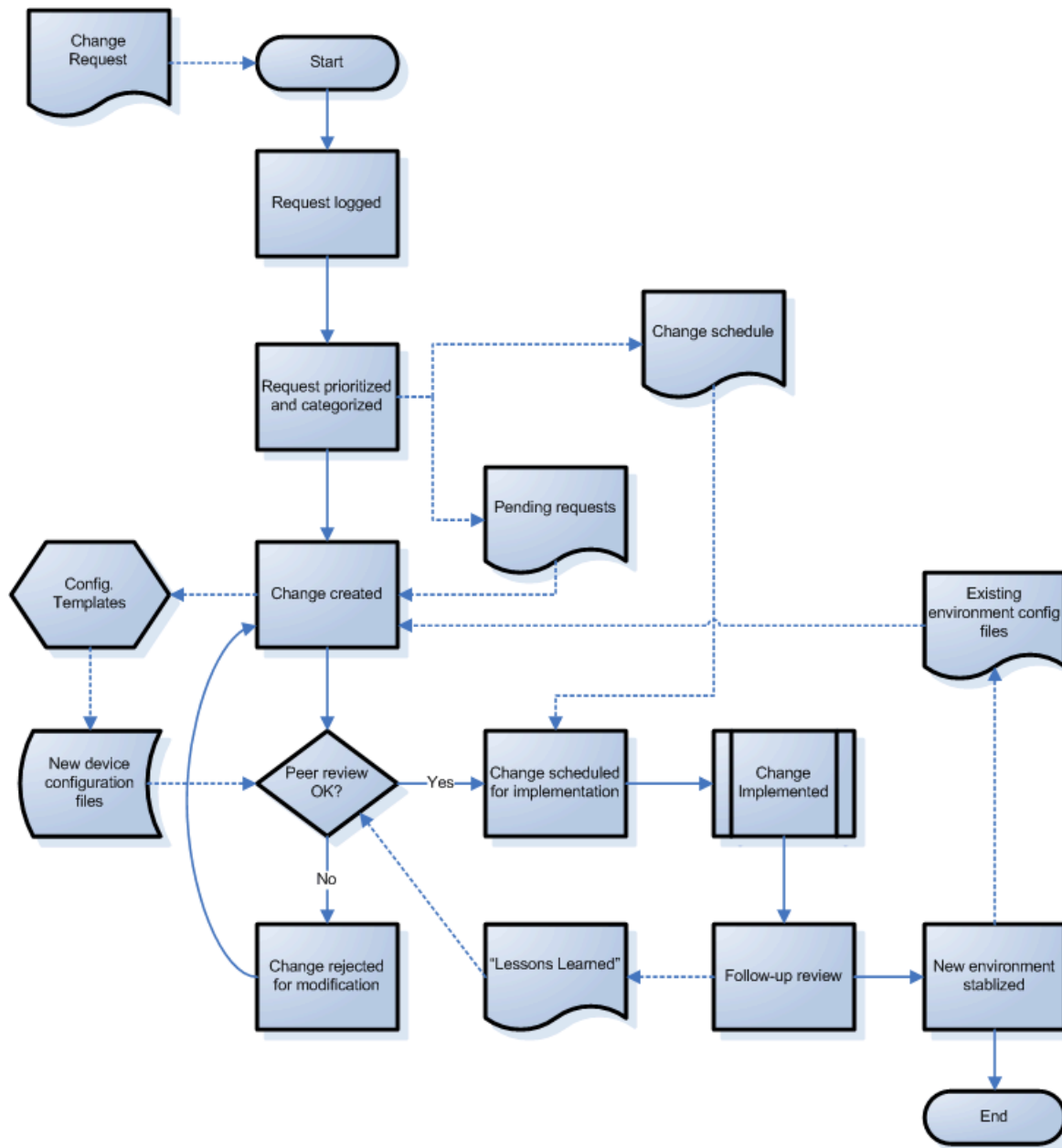
## Industry Best Practices

What should your change-management process incorporate? Which best practices have evolved in the IT industry that you can leverage to create an effective process? Chapter 7 will focus almost entirely on best practices, but the following list provides an overview of what your process should address:


- **Change logging and filtering**—Your process must include formal documentation for change requests. You should also spell out exactly who in your organization is permitted to submit change requests (ideally, everyone should be permitted to submit requests). Making the process accessible to everyone encourages participation; locking down the process encourages vigilantes who try to circumvent the process.
- **Provide links between problems and changes**—When requesting a change to resolve a problem, ensure that the change request and the original problem remain linked in some fashion. Doing so will provide built-in documentation for the reason behind the change and provide information that can be used in post-change analysis.
- **Multiple priorities**—Given that you can only accomplish so much in a day, your process needs to accommodate changes that are more important than others. Some initial review of change requests needs to occur shortly after their receipt so that the requests can be “triaged” and fed to the remainder of the process according to priority. Above all, ensure that your process doesn't create artificial barriers in the way of legitimate changes that are necessary for business or stability purposes. Your goal should be to create a usable management process, not an artificially complex bureaucracy.
- **Multiple categories**—Build your process to acknowledge different types of change requests. You might categorize changes by the risk they pose to your environment, the resources required to deploy the change, the complexity of the change, or some combination of these and other factors. Categories should serve a useful purpose in helping to prioritize and manage changes.

- **Review**—Your process must incorporate some type of review process to ensure that changes will be effective and safe. Total Quality Management (TQM) principles suggest that peer reviews are the best: studies have shown that professionals in most industries pay more attention to their work when they know a peer will be reviewing it. Supervisory review and signoff may be a political requirement in your organization, but this step is not a technical review. Don't rely on the hope that the boss is going to pick up on technical problems with a proposed change.
- **Periodic focus meetings**—To ensure that everyone involved with the change-management and implementation process remains focused, schedule periodic focus meetings. Held once a month or once a quarter, these meetings allow the team to discuss problems with the process and to discuss long-term changes that are in the works. These meetings can also serve as a forum for discussing failed changes so that each member of the team can learn the lesson the mistake offers.
- **Approval**—In the end, your process must include some formal approval step through which changes are approved and schedule for implementation.
- **Follow-up**—Your process should also include a follow-up review of each change, either at a focus meeting or by a senior administrator. This review should frankly assess any negative impact created by the change, and these reviews should be fed back into the change-management process to fine-tune that process and prevent future problems of the same kind.

Figure 1.7 shows a generic change-management process that incorporates many of these elements. The documentation that is produced as a part of the process and how some of those documents—such as the “lessons learned” document created in the follow-up steps—are used as review checklists when examining future change requests.



**Figure 1.7: A generic change-management process.**

 In these flowcharts, solid lines represent the actual process flow. Dotted lines represent information or data that is placed into documents (or other forms of storage) or information and data from documents that is utilized in a step of the process.

## What Else Do You Need to Know?

Plenty—and I'll explain it all in the next seven chapters. My goal is to provide you with a complete, detailed description of every aspect of change management. I'll also provide tips for creating your own process and fitting it to your environment.

### ***Network Change Management and Stability***

In Chapter 2, I'll start by describing the effect that change management can have on business performance. I'll look at a couple of short case studies from my consulting practice in which change management had a definite impact on the business' overall stability. I'll also outline the steps for creating a formal process for change, including:

- Reviewing and approving proposed changes
- Prioritizing change
- Assigning and compensating for risk
- Monitoring pending changes
- Documenting and archiving changes

I'll also talk about *rollback*, the process of undoing a change that caused problems. Even with the most rigorous change-management process, it is possible for your changes to go awry; perhaps there were factors outside your control that you didn't account for or a bug in a device's firmware reared its ugly head. Regardless, any good change-management process will include a process for backing out of a change and restoring things to working order as quickly as possible.

### ***Network Change Management and Security***

How can network change management affect network security? *Any* unplanned change is a security incident. Even changes that have been authorized but not yet planned for are a security problem. Without a change-management process in place, you'll never know when unauthorized changes occur—and even with a solid plan in place, you will still need to prepare an incident response.

Fortunately, change-management processes can be supported by a variety of tools that provide for real-time monitoring and logging of changes, instant rollback to undo unauthorized changes, and detailed auditing to track changes made on network devices.

I can't stress enough the importance of bringing security to network management. Government regulations—such as the Health Insurance Portability and Accountability Act (HIPAA), CFR 21 Part 11, and the Gramm-Leach-Bliley Act—all place an incredible burden on specific industries to maintain secure, accountable environments. Companies in these industries spend literally millions of dollars coming into compliance with the laws, and don't often realize the gaping vulnerability that their network management practices can represent.

## **The Scope of Change Management**

Change management isn't a process or a technology, it's a mental state and company philosophy. You could probably sit down with a big sheet of paper and a pen and come up with the perfect change-management process. Unfortunately, implementing that process might be difficult simply due to the current state of technology. There are only so many change-management tools available, and, more important, network devices don't always lend themselves to effective change management. In fact, most change-management tools currently on the market are amazing primarily for their ability to work around the limitations of the devices they're managing.


In Chapter 4, I'll discuss the scope that you can expect from a change-management process. I'll describe integration with systems such as Hewlett-Packard OpenView, and discuss the management capabilities for routers, switches, firewalls, load balancers, virtual private network (VPN) concentrators, intrusion detection and prevention devices, and more. I'll also take a brief look at how servers can be included in your network change-management strategy, including UNIX- and Linux-based servers, Windows servers, Novell servers, Windows PCs, UNIX- and Linux-based workstations, and so forth.

## **Network Change-Management Technologies**

Change management is definitely a state of mind, but it is also something you can realistically implement in your environment, thanks to a bevy of supporting technologies:

- Simple Network Management Protocol (SNMP)
- Syslog
- SSH and SSL
- Trivial File Transfer Protocol (TFTP)
- Telnet
- Remote Authentication Dial-In User Service (RADIUS), and its cousins TACACS and TACACS+

These technologies are the underlying enablers of many change-management tools, and they each have caveats and concerns, particularly with regard to security. Although good change-management tools provide a fairly secure setup, you will benefit from knowing how they might be used to attack other parts of your network. I'll devote all of Chapter 5 to discussing these technologies, explaining how they work, and explaining their role in change management.

 Many of these technologies, combined with good old fashioned command-line scripts, can be used to provide rudimentary change-management capabilities until you get proper tools in place. For example, you can write scripts that utilize TFTP to regularly pull device configuration files, then use diff or other command-line file-comparison tools to generate a file that contains the differences between two versions of a configuration file. It's far from automatic, but it's a technique that has served many organizations until they get proper processes and tools in place.

## **Network Change-Management Tools**

I've used the term *network change-management tools* a dozen times so far in this chapter; what are they? Generally, a suite of tools is required to provide full end-to-end functionality. For example, you might start with a Help desk call tracking system that can track both problems as well as change requests. Other tools make it easier to plan for changes by allowing you to review the changes and implement workflows such as peer reviews and management approval. Other tools can be used to actually deploy changes (making it easier to roll out late-night changes while still getting some shut-eye) and to archive changes for future analysis and possible rollback. Most tools support a proactive change-management process, which is a much more mature way of managing your network.

For the various categories of tools, I'll provide some selection criteria to give you an idea of what is available in the marketplace so that you can look for solutions that meet your organization's needs. Some of the types of tools I'll cover include:

- Problem tracking
- Knowledge bases
- Management reporting
- Change rollback and recovery
- Change archival and tracking
- Change deployment and implementation
- Change modeling and risk analysis
- Environment inventory and review
- Accepting and tracking change requests
- Designing and staging complex multi-device changes

## **Network Change-Management Best Practices**

Which processes work best for you? What are other companies doing? Where do you start and how will you know you've finished creating a good process for change management? All tough questions, especially if your organization hasn't traditionally worried much about change management. Fortunately, you're not alone: a number of industry best practices exist that describe what a good change-management process should take into account. I'll introduce you to these best practices, focusing on the Information Technology Infrastructure Library (ITIL), a set of IT-wide best practices that includes a specific set of practices for managing change.

## Sample Change-Management Processes

Finally, in Chapter 8, I'll provide you with some sample change-management processes. For each, I'll provide complete workflow charts and step-by-step descriptions. You should be able to use these as a starting point for developing your own processes, and for each one I'll point out steps where various tools and technologies can be implemented to help automate or improve those steps. Some of the processes I'll provide include:

- Basic change management for a small IT shop
- Change management processes that incorporate peer review
- Processes that incorporate both peer review and supervisory review and approval
- Shared management processes, which typically apply to situations in which a customer engineers their network but outsources daily operations
- Shared management processes in which the customer outsources both engineer and operations but retains oversight and approval
- Processes that focus on security, using a comprehensive audit as the starting point, followed by the creation and use of design templates used to enforce both consistency and security

You should be able to mix and match these processes to achieve something that works well for just about any organization.

### IBM and Hewlett-Packard's Enterprise Management Initiatives

Both IBM and HP have recently announced new management initiatives that the companies say will help make business and IT more tightly linked and will make IT more responsive to business' need for flexibility and rapid evolution. IBM's offering is called *OnDemand* and HP's is called *Adaptive Enterprise*. Although both companies are still positioning the products and services that comprise their initiatives—because they're not just products and not just consulting services—one thing is for certain: change management is a major part of their philosophies.

The traditional danger in making fast changes to IT infrastructure, software, and support has been that unplanned change results in chaos. You've seen it yourself: the new line-of-business (LOB) application that never got properly deployed or the new enterprise management software that failed during implementation. Even companies such as Microsoft were victims to too much change: the day Microsoft released Windows XP, it also released nearly 20MB of patches for it.

Proper change management is a key to making IT more flexible. By understanding how change is evaluated and implemented and by having a well-understood process to support change, changes to the entire infrastructure can be made confidently and safely. Enterprise-class companies such as IBM and HP recognize this, and are making change management an important part of the service and product offerings they are creating to help their customers.



## Summary

Change management is something that many industries have used for years. For example, if you've ever built a house, you know full well the impact a seemingly minor change request can have. An architect has to decide how the change might be incorporated into the overall design, and an engineer has to ensure that it won't compromise the overall structure. An inspector may have to issue a variance or permit to incorporate the change, giving the local government the opportunity to conduct what amounts to a peer review. Workers' copies of blueprints and other documents—the housing equivalent of a device configuration file—must be updated and distributed. You and your builder have to follow up on the change's implementation to ensure that it won't create any cascade effects in the rest of the process, and ensure that the change was incorporated properly.

There's no reason why the IT industry can't make the same effective use of change management when managing networks. With the right process, the right tools, and the desire to reduce the potentially devastating operational and financial impact of unplanned change, change management can easily become an effective, productive part of your network. In the next chapter, I'll dive right in with a more detailed look at the precise impact change management has on the network and the tasks that change-management processes must incorporate and address.