

Realtime  
publishers

"Leading the Conversation"

# *The Shortcut Guide<sup>™</sup> To*



# Automating Network Management and Compliance

*sponsored by*



i n v e n t

*Don Jones*

---

## Introduction to Realtimepublishers

by Sean Daily, Series Editor

The book you are about to enjoy represents an entirely new modality of publishing and a major first in the 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 technology topics—at no cost to the reader. Although this feat may sound difficult to achieve, it is made possible through the vision and generosity of a corporate sponsor who agrees 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 publications does not in any way diminish their quality. Without reservation, I can tell you that the book that you're now reading 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. The Realtimepublishers publishing model also provides other significant benefits. For example, the electronic nature of this book makes activities such as chapter updates and additions or the release of a new edition possible in a far shorter timeframe than is the case with conventional 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 our books are by no means paid advertisements for the sponsor. Realtimepublishers is an independent publishing company and maintains, by written agreement with the sponsor, 100 percent editorial control over the content of our titles. It is my opinion that this system of content delivery not only is of immeasurable value to readers but also will hold a significant place in the future of publishing.

As the founder of Realtimepublishers, my *raison d'être* is to create “dream team” projects—that is, to locate and work only with the industry's leading authors and sponsors, and publish books that help readers 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 send an email to [feedback@realtimepublishers.com](mailto:feedback@realtimepublishers.com), leave feedback on our Web site at <http://www.realtimepublishers.com>, or call us at 800-509-0532 ext. 110.

Thanks for reading, and enjoy!

Sean Daily  
Founder & Series Editor  
Realtimepublishers.com, Inc.

Introduction to Realtimepublishers..... i

Chapter 1: The Essentials of Automating Network Operations.....1

What Is Automation? .....1

The Price of a Non-Automated Network .....3

    Inconsistency.....3

    Security Breaches.....5

    Downtime.....6

    Inability to Respond to Business Demands .....7

    Lack of Business Reliability .....8

    Loss of Customer and Investor Confidence.....8

    Lack of Efficiency.....8

Your Network’s Challenges.....9

    Poor Administrative Practices.....9

    Technical Attacks.....10

    Social Engineering .....11

    Physical Disaster and Other Elements Outside Your Control .....12

    Process Adherence .....12

The Benefits of an Automated Network .....14

    Configurable .....14

    Consistent.....15

    Recoverable.....15

    Securable.....16

    Compliant.....18

    Auditable.....19

    Efficient.....19

    Flexible .....19

Traditional Management vs. Automated Management.....20

    Ad-Hoc Configuration .....20

    Manual Backup and Recovery .....22

    Scripted Administration .....23

Summary .....23

## Copyright Statement

© 2005 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.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 Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.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.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

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



[**Editor's Note:** This eBook was downloaded from Content Central. To download other eBooks on this topic, please visit <http://www.realtimepublishers.com/contentcentral/>.]

## Chapter 1: The Essentials of Automating Network Operations

Modern computer networks are an absolutely mission-critical part of almost any business. Yet because the network doesn't do anything visible—most users, that is, are more focused on services such as email or file sharing than on the network that makes these services possible—the network's critical role is often overlooked or diminished. However, the important role the network plays in the business has a very significant impact on the business' efficiency, overall operations, and the bottom line. This guide explores the ways in which a more efficient, more automated network can lend significant value to the business in a number of different areas.

### What *Is* Automation?

**au•to•ma•tion** *n.*

1. The automation operation of control of equipment, a process, or a system.
2. The techniques and equipment used to achieve automatic operation or control.
3. The condition of being automatically controlled or operated.

- *The American Heritage Dictionary of the English Language, Fourth Edition*

Automation seems like a strange term to apply to network operations. After all, at first glance, networks don't seem to offer much in the way of manual operation. Routers already route packets automatically, for example. A technology such as Dynamic Host Configuration Protocol (DHCP) might seem to be a beneficial form of network automation, but not much else immediately comes to mind.

Network operations, however, are in fact a *tremendously* manual process in most companies. The provisioning, configuration, ongoing maintenance, disaster recovery, and other tasks involved in managing the network are typically accomplished entirely through manual effort, or (too often) inefficiently automated through cobbled-together techniques. In many companies, every change made to the network's configuration—from modifying a router's routing table to backing up the configuration of a switch—is made manually. Recovery of failed devices is performed manually. *Everything* needed to keep the network up and running, in many companies, is done manually. But by automating network operations—that is, by automating day-to-day changes, a change management workflow, disaster recovery operations, and other tasks related to network management—companies can realize significant business benefits.

To help you do so, this chapter will explore the essentials of automated network operations: The real business costs of a non-automated network, the benefits offered by automation, and a comparison of automated versus more traditional management techniques.

The next chapter will look at network compliance and security from an automation viewpoint, focusing on how compliance affects the network, how automation can affect security and compliance efforts, and how traditional—that is, largely manual—management techniques leave loopholes in security and compliance management efforts. This chapter will also look at how various technologies and tools can be used to close those loopholes to create a more secure, more compliant network. Chapter 2 will also look at auditing, and explore the differences between various auditing philosophies and how network automation can be used to make auditing easier and more efficient.

Chapter 3 will explore ways in which automation can help improve the network’s operational efficiency and increase the network’s overall availability, or uptime. This chapter will explain the important differences between commonly sought-after disaster recovery goals and the more desirable business continuity goals, and the challenges that exist to a network’s overall availability in a traditionally-managed and -operated network. Chapter 3 will help you develop a business process for maximizing network availability, and look at some of the core technologies that make a high-availability network a possibility. I’ll also help you understand how all-in-one network configuration management solutions can improve uptime through automation, and how they can respond to various business continuity scenarios and challenges with ease.

Finally, Chapter 4 will help you put together a complete plan for automating your network operations tasks. It will start with the supporting business processes, helping you adapt frameworks such as the Information Technology Infrastructure Library (ITIL), and continue with how to examine and evolve your current business processes. Because tools and technologies play such an important role in network automation, this chapter will help you develop a solution evaluation project and list of criteria that works for your business so that you can evaluate various tools and technologies and identify the ones that work best for you. The chapter will then show you how to integrate your new business processes and whatever solution you select to create a complete, “closed loop” system for automated network operations. The guide will finish by covering core business plans for daily network administration, security and compliance auditing, and disaster planning.

This guide has a lot of ground to cover—I’ll keep everything moving quickly so that you can begin implementing a more efficient, more automated network right away. Let’s start, however, by clearly identifying the real business costs of an old-fashioned, non-automated network.

## The Price of a Non-Automated Network

Many network managers and engineers don't realize that a manually operated network carries a number of significant risks and business costs. Often, an automated network is seen as a convenience to the engineers and technicians who run the network; in fact, an automated network provides significant value directly to the business. Of course, that means a non-automated network detracts significant value from the business, and comes with real, tangible costs. The next several sections will discuss some of those costs and how they can negatively impact the business.

### Inconsistency

Inconsistency is a major problem for any network. For example, consider Figure 1.1, which shows two router configuration files side-by-side in Windows Notepad. Both configuration files are intended for use on the same or similar routers; can you spot the differences?

```

Untitled - Notepad
File Edit Format View Help
version 10.3
!
hostname blah.test.org
!
enable secret 5 (#>30u34(#(%)_$%*#!_BIEWQBMX
enable password passwordhere
!
ip subnet-zero
!
interface Ethernet0
 ip address 5.5.5.5 255.255.255.128
 no ip directed-broadcast
!
interface Serial0
 description Gateway to Internet provider
 ip address 4.4.4.4 255.255.255.252
 no ip directed-broadcast
 encapsulation frame-relay IETF
 no ip route-cache
 bandwidth 1536
 frame-relay lmi-type ansi
!
interface Serial1
 no ip address
 shutdown
!
ip classless
 ip route 0.0.0.0 0.0.0.0 4.4.4.3
 banner login AC
 -=welcome to the main gateway=-
 AC
!
line con 0
 password passwordhere
 login
line aux 0
 transport input all
line vty 0 4
 password passwordhere
 login
!
end

Untitled - Notepad
File Edit Format View Help
version 10.3
!
hostname blah.test.org
!
enable secret 5 (#>30u34(#(%)_$%*#!_BIEWQBMX
enable password passwordhere
!
ip subnet-zero
!
interface Ethernet0
 ip address 5.5.5.5 255.255.255.128
 no ip directed-broadcast
!
interface Serial0
 description Gateway to Internet provider
 ip address 4.4.4.4 255.255.255.252
 no ip directed-broadcast
 encapsulation frame-relay IETF
 no ip route-cache
 bandwidth 1536
 frame-relay lmi-type ansi
!
interface Serial1
 no ip address
 shutdown
!
ip classless
 ip route 0.0.0.0 0.0.0.0 4.4.4.3
 banner login AC
 -=welcome to the gateway=-
 AC
!
line con 0
 password passwordhere
 login
line aux 0
 transport input all
line vty 0 4
 password passwordher
 login
!
end

```

Figure 1.1: Comparing router configurations.



These are *simple* configuration files, dozens of times shorter than the one a production router might usually contain. There are two inconsistencies here: The first is in the login banner, “Welcome to the main gateway,” which simply says “Welcome to the gateway” in the second file. There is no real harm in that type of inconsistency. The second inconsistency, however, is more serious: The password for the “line vty” interface, near the bottom of the files. Inconsistent security settings means inconsistent network access. Some devices may be more secure than others. Inconsistencies can cause one device to operate and another, similar device, to fail. It can interfere with the operation of the network and waste hours in frustrating troubleshooting. Other configuration inconsistencies can make devices behave more or less efficiently than others, and make them more or less difficult to manage. Inconsistent configurations are a hallmark of manually configured networks, simply because human error makes it nearly impossible for manual changes to be made consistently on any kind of large scale. Although devices might start out consistently configured (perhaps using a template of some kind as a starting point), every manual change made to a device increases its deviation from that initial standard and increases the amount of inconsistency in the network.

The business costs of inconsistency include:

- Lowered security—In a large device configuration—such as a firewall or perimeter router—it’s extremely easy for minor inconsistencies to go overlooked in a manual review. It’s also easy to introduce minor inconsistencies when making changes manually. However, minor inconsistencies—such as an incorrectly opened port—can result in vastly decreased overall security. In companies dealing with compliance requirements, lowered security can result in a failed compliance audit, with the associated costs. Regardless, lowered security opens the door to very real business losses.
- Less manageability and less flexibility—An inconsistently configured network is more difficult to manage. When making configuration changes, devices must be carefully reviewed by skilled (and expensive) engineers to ensure that the new change won’t negatively impact the device or the network. With each device configured differently—that is, inconsistently—this review takes longer and is more error-prone because small details are likely to be overlooked. As a result, every change to the network becomes more difficult and risky. Businesses often deal with this risk through avoidance, meaning changes to the network are discouraged. This method leads to a network that is less able to respond to changing business requirements, keeping the business from evolving and remaining competitive.
- Less recoverable devices—When devices are inconsistently configured, recovering a device after a failure becomes riskier because there is no one standard that describes how the device was configured. Thus, downtime lasts longer, as devices’ inconsistent configurations are more painstakingly recreated. Downtime equals lost money for the business.

There is no question that inconsistently configured networks present significant business risks, both short- and long-term. There is also no question that a manually configured network is more likely to contain these inconsistencies, increasing the chance that the network will detract value from the business rather than adding value.

## Security Breaches

Security breaches are a major concern for any business. The risk of losing proprietary intellectual property, personal identifiable information, and other confidential data—and thus losing money as well as customer and investor confidence—is well understood. At the network level, security breaches are made possible through unpatched devices, improperly configured devices, and poorly configured devices (devices that have, for example, old or inappropriate Simple Network Management Protocol—SNMP—community strings, thus leaving themselves open to unauthorized reconfiguration). Manually configured networks exhibit some common characteristics and management practices that make security breaches more likely:

- **Unpatched**—Deploying patches can be a nightmare, especially on large networks, so overworked engineers and administrators are often well behind the curve in deploying patches to devices. However, because patches often fix security issues and other vulnerabilities, unpatched devices are a major security risk.
- **Poor practices**—Network security elements such as configuration passwords, SNMP community strings, and so forth should be changed on a regular basis, just like network user passwords. However, *rolling passwords*, as they are called, are a major undertaking in a manually configured network. Most companies simply ignore the security risk and accept poor practices as a way of life.
- **Time**—The sheer time involved in manually configuring devices often leads harried administrators to not implement deep defensive measures which, were they in use, could help stop a broader range of attacks.
- **Unauthorized changes**—Manually configured networks are open to problems with process adherence. In other words, businesses may have a thorough configuration management process in place, but a manually configured network provides a number of loopholes to these processes, allowing administrators to make “one minor change” here and there, outside the process. These changes, bypassing as they do the process review and approval stages, are more likely to open security holes in the network that go undetected for a significant period of time.

### Why Are Network Devices Vulnerable?

Some network managers and engineers don't believe that their devices are vulnerable. An infrequently changed SNMP community string, they feel, doesn't present a risk because the device itself is behind a firewall, thus preventing—or so they believe—an attacker from taking advantage of any vulnerability. Likewise, unpatched devices aren't viewed as a risk because there's "no way" for an attacker to access the device and exploit any vulnerabilities.

However, that viewpoint is naïve. *Most* attacks on corporate resources come from *within* the firewall, either from internal attackers (such as disgruntled employees) or from malicious software (such as viruses) that make it into the intranet through users' removable media drives or other means. The idea that the intranet is somehow inherently safe is completely false, and creates a false, and highly inappropriate, sense of security. The intranet is *not* safe.

Therefore, best practices suggest changing SNMP community strings, device configuration passwords, and other security elements on a frequent (often every 30 to 45 days) basis. In addition, best practices—and device manufacturers—recommend applying the latest device software patches as quickly as possible, particularly for patches that repair a security vulnerability. Ignoring these practices invites attack, with all the very real costs that a successful attack can introduce to the business.

Of course, these best practices are often difficult and even risky to perform manually. For example, what if a device's SNMP community string or configuration password is input improperly? The device becomes unmanageable. These reasons highlight why network automation is crucial and why a manually configured network offers so many costs in terms of poor security.

### Downtime

Most businesses are well aware of the costs of downtime, but most don't realize the degree to which a manually configured network makes downtime both more likely and longer in duration. Simply put, manual changes are error-prone. One Cisco study found an error rate of 5 percent for manually performed changes; in a network with just 100 devices, that means five of those devices will be improperly configured at some point. Because of the precise nature of network device configuration, a single error can result in partial or total network service outages. Simply planning a single minor change to every device on the network will, statistically, result in five of them being changed incorrectly and therefore introducing at risk for downtime. That risk, by the way, is why so many manually configured networks avoid deploying patches, changing device passwords and other security elements, and so forth—error, and potential downtime, is practically inevitable.

Once downtime does occur, a manually configured network is more likely to have a longer downtime. The reason is that device configuration backups must be manually made, as well, with the same error rate and likelihood of someone forgetting to make the backup. Restoring the device configuration is also a manual process, requiring the correct backup configuration to be located, manually loaded into the device (meaning someone may have to look up the proper device access passwords first, yet another delay), and so forth. An informal study with a consulting client found that the average manual recovery time for a network device was 30 minutes. In some businesses, literally millions of dollars can be lost in 30 minutes if the network isn't available.

## ***Inability to Respond to Business Demands***

With all of the problems—inconsistency, downtime, security issues, and more—that a manually configured network can present, it's no surprise that most companies adopt a strict policy regarding network changes: They perform the changes only if they are absolutely necessary. The idea is to reduce the risk of inconsistency, downtime, security problems, and so forth, and that severely limiting change will, in fact, reduce that risk. In many shops, the very word *change* is a bad one, and engineers will share horror stories of the supposedly minor change that took the company down for an entire day.

But modern business is *about* change. In order to remain competitive, businesses need the flexibility to adapt quickly to changing market conditions, and that often means changing the network as well. Companies such as Hewlett-Packard, IBM, and Microsoft are all touting frameworks and technologies that enable rapid change (Adaptive Enterprise, OnDemand, and Dynamic Systems Initiative, respectively) because smart businesses realize that flexibility is one of the most important competitive advantages they can possess. Restricting network change because of the risk of change itself artificially limits what the business can do to remain competitive; this limits the business' growth, frustrates employees, and hinders investor confidence.

Most companies don't see themselves as inflexible. However, almost any employee at any company can tell you about the workarounds they're forced to take simply because the IT staff isn't capable of providing the proper services. Some examples from a recent client include:

- Employees were sending confidential materials to business partners through free email services such as Yahoo and GMail. The corporate email system prevented these materials from being sent, and the network staff didn't want to create any kind of extranet or other connectivity options.
- Several new services needed to be implemented that required changes to the corporate firewall. However, permanent firewall changes were limited to a once-per-quarter scheduled change period, meaning the company simply had to wait 3 months for the needed changes to be implemented.
- The company failed a compliance audit because device configuration passwords hadn't been changed. Network managers had determined that the yearly cost of changing passwords would be in the neighborhood of \$5184 and require 103 hours per year; they had decided it would be cheaper not to do so. As a result of the failed compliance, the company was delayed 6 months in an initial public offering.

In almost every case, the reason for the lack of a real solution was because the network infrastructure team didn't want to make the necessary changes because changes required too much advance planning, too much effort to implement, and too frequently created additional issues. As a result, they strictly limited changes—and thus limited the business.

### **Lack of Business Reliability**

What is a reliable business? A business upon which customers and employees can depend. If you work for a bank and network infrastructure issues take your self-service banking Web site offline for a day, customers complain and feel you're unreliable. If you work for a hospital and a network failure makes patient data unavailable for a few hours, customers could *die*. Any kind of network failure can result in public impact and make customers—and even employees, in the case of purely internal failures—view your business as unreliable. People don't like to do business with, or work for, unreliable businesses. If you're viewed as unreliable, people find someone else with which to do business, or someone else to work for. The cost of this perception and its associated losses are difficult to precisely quantify but are very real nonetheless.


A network that is consistently configured, well-secured, and highly available can help bring more reliability to your overall business. A network that's inconsistently configured, poorly secured, and that experiences downtime is a network that makes your business unreliable, and unreliable businesses don't last long.

### **Loss of Customer and Investor Confidence**

Inconsistency, security issues, downtime, inflexibility—these are mainly internal issues that external observers won't see directly. But the results of these issues can cause a significant loss in customer and investor confidence. For example, if your company's poor network security results in a loss of intellectual property, your stock price could fall through the basement and customers—wary of entrusting you with their own personal information—could stay away in droves. Witness the public relations nightmares that financial services firms have had when credit card holder information was stolen over the Internet. In a competitive marketplace in which consumers are always a step away from going to the competition, this sort of failure can ruin a business for years, if not permanently.

### **Lack of Efficiency**

Suppose you have a network with 800 devices and that an administrator can manually change device passwords, when the time comes, at the rate of about 1 per minute—a task the administrator performs once per quarter—which is a long time to go between password changes. This task results in about 95 hours per year. Let's also say that you spend about 300 hours per year deploying patches to those 800 devices (not unreasonable; that allows about 10 minutes per patch and just 2 to 3 patches per device for an entire year), and another 90 hours gathering configurations from devices (for backups and so forth). These tasks add up to about 485 hours per year of network management, which can run into some pretty significant monetary costs, just in terms of administrator salaries. And that is just for some very minimal administrative tasks—not even the complete scope of what an administrator would actually do all year.

 Automating these tasks reduces the numbers to about 30 hours for patch deployment, 15 minutes for configuration backups, and about an hour for password changes—*per year* (numbers based on estimates by both Cisco and Nortel). That is a lot of savings just in administrator time (and the associated salaries): Your administrators will have a lot more time to work on other projects as a result. This automation can also allow you to reduce the number of staff or contractors, and make a really significant impact on the bottom line. True, you'll spend some money on tools and technologies to achieve this automation, but the savings are significant. And keep in mind that I've only touched on the tip of the iceberg with this illustration. In reality, your network administrators will save time on almost every device-related management task, and that time will translate into some pretty significant monetary savings.

Automating network operations increases efficiency. Increased efficiency results in monetary savings. It's a pretty simple formula.

## Your Network's Challenges

It's important to understand the challenges that your network faces. These are the things that make manual network operations so dangerous and can compromise a manual process and cost your business money, public confidence, and resources. Let's explore how each challenge can result in problems within a manually configured network and how automation of various kinds can help mitigate the challenge and remove the risk.

### **Poor Administrative Practices**


Poor administrative practices are one of the biggest dangers faced by the network. Ad-hoc, poorly, or insufficiently planned changes are the ones most likely to result in downtime, insecure configurations, and so forth. The only way to eliminate poor administrative practices is to have a well thought-out configuration and change management process in place. Such a process helps to ensure changes receive the appropriate amount of planning and review to prevent problems. Of course, simply *having* a process doesn't guarantee its *use*; the problem of process adherence is a real one that I'll discuss shortly.

Another poor practice that challenges your network relates to security. Tasks such as patch management, password changes, SNMP community string changes, and so forth are all critical operations for a secure, reliable, compliant network, although many companies accept poor practices by not deploying patches in a timely fashion, failing to change passwords, and not changing SNMP community strings. The only way to improve these poor practices is to make a conscious effort to do a better job. Unfortunately, the risks associated with better practices—such as the risk of error when rolling passwords or the risk of failure when deploying a patch—can be significant. Automation can help reduce the risks by improving the consistency of changes and by providing a rapid and even automated recovery when a patch deployment goes wrong.

## Technical Attacks

Your network is *always* at risk from technical attacks: Denial of Service (DoS) attacks, exploits of unpatched security vulnerabilities, and more. Best practices—such as frequent password changes, conscientious patch management practices, and so forth—can help reduce the likelihood of a successful technical attack. Automation makes these best practices easier to implement by helping make password changes and patch management more efficient, less error-prone, and more automatic.

Another way technical attacks often succeed is through improper configuration settings. For example, a new administrator might accidentally configure a router using a configuration template, similar to the one that Listing 1.1 shows. The use of such templates is normally a good idea, as they can be used to ensure consistent initial configurations of devices.

 This configuration is excerpted from a more complete one offered by Rob Thomas at <http://www.cymru.com/Documents/secure-ios-template.html>.

```

! Use TACACS+ for AAA. Ensure that the local account is
! case-sensitive, thus making brute-force attacks less
! effective.
aaa new-model
aaa authentication login default group tacacs+ local-case
aaa authentication enable default group tacacs+ enable
aaa authorization commands 15 default group tacacs+ local
aaa accounting exec default stop-only group tacacs+
aaa accounting commands 15 default stop-only group tacacs+
aaa accounting network default stop-only group tacacs+
tacacs-server host 7.7.7.5
tacacs-server key cheezit
!
! In the event that TACACS+ fails, use case-sensitive local
! authentication instead. Keeps the hackers guessing, and
! the router more secure.
username <USERNAME> secret <PASSWORD>
!
! Don't run the HTTP server.
no ip http server
no ip http server-secure
!
! Allow us to use the low subnet and go classless
ip subnet-zero
ip classless
!
! Disable noxious services
no service pad
no ip source-route
no ip finger
no ip bootp server
no ip domain-lookup

```

**Listing 1.1: An example configuration template.**

However, templates are static files often kept on individual administrators' workstations, making them unreliable as an authoritative configuration model. In this case, suppose the new administrator had obtained an older version of the template, not realizing that the TACACS+ server addresses had changed. Deploying this template would leave the device open to potential attack, as the old address could now possibly be used by an unauthorized TACACS+ server, thus providing a means by which an attacker could compromise the router's security.

An automation solution could help prevent this type of problem by analyzing all proposed changes against a set of centrally configured policies. When the configured TACACS+ server address doesn't match the solution's central policy, the change could be flagged or rejected outright, preventing it from being applied to the device and therefore preventing a potential attack. In fact, almost any type of configuration problem of this nature can be avoided through an automated configuration management solution that supports the use of policies as a check on new configurations.

**Social Engineering**

What is social engineering?

“Hi, this is the head of research. I need you to open an incoming firewall port for a project we're working on. I just need it open for a couple of hours. I'll send the authorization later. Can you do this for me now?”

Thus begins a social engineering attack: Exploiting the weak link—the people—in any process to bypass safeguards. An automated configuration management solution can, depending on the solution itself, help prevent this type of attack in a number of ways.

- **Process adherence**—By forcing administrators to make changes in accordance with a process, ad-hoc changes such as this become more difficult to make. The change can be tracked and rolled back, and the solution can be configured to require secondary authorization by a manager or peer. The greater number of people that have to be manipulated, the less likely the attack is to succeed.
- **Tie-in**—Tie-in is the idea of having a “closed-loop” configuration management system. Changes can only be deployed if they're matched to a request in a Help desk ticketing system, thus ensuring that requests such as this have to go through proper channels and thus reducing the opportunity for a socially engineered bypass to the process.
- **Policy enforcement**—If the configuration solution provides policy support, a central policy can be configured that details what changes are allowed, especially with regard to sensitive configurations such as open ports in a firewall. Changes outside the policy are rejected. A change request such as this one would have to start with a change to the policy itself, which typically wouldn't be accessible to a front-line administrator, thus defeating the social engineering attempt.



## **Physical Disaster and Other Elements Outside Your Control**

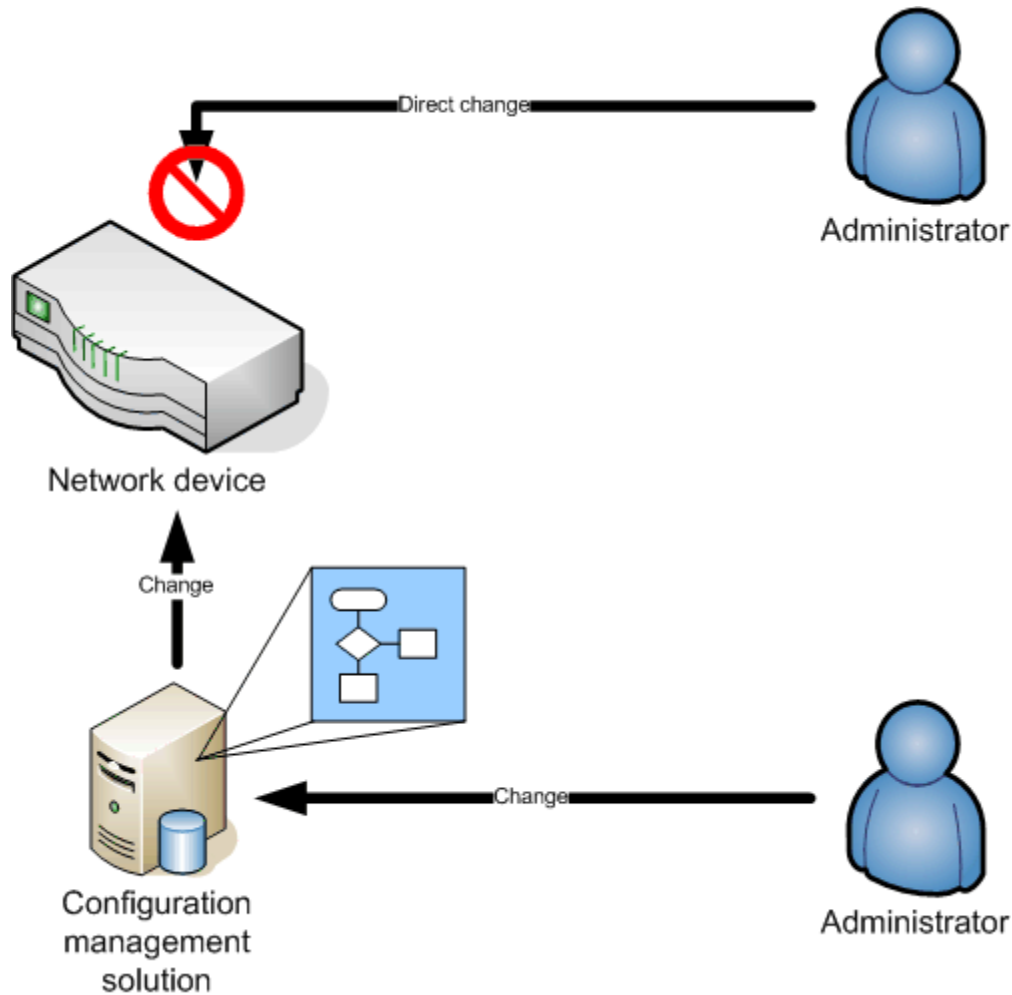
All networks are subject to acts of nature: flood, fire, or simple failed electronics. Although no amount of automation can *prevent* these problems on your network, automation can help significantly reduce their impact. For example, in the event of a failure, an automated configuration solution can be used to quickly deploy a failed device's configuration to a backup device, restoring service much more quickly than a manual reconstruction could. In the event of a natural disaster, an automated configuration solution can be used to restore multiple devices' configurations to backup devices located at an offsite recovery facility, decreasing the time it takes to get the remainder of the business functioning at the backup facility.

Whether your network fails because of an earthquake or because of a simple, temporary failure in utility power, having an automated network configuration management solution can make the recovery process much faster. The automated solution can be configured to routinely back up device configurations, ensuring that your configuration repository *always* has the latest and greatest operational configuration—something that manual configuration management processes often fail to do consistently—and can push out configuration files to dozens or hundreds of devices simultaneously, vastly reducing the time it takes to get the network back up and running.

## **Process Adherence**

Many of the challenges I've discussed to this point can be solved, or at least highly mitigated, through a well thought-out process. But processes only go so far; a flowchart alone can't force your network to become more secure, more efficient, and more reliable. In this arena, an all-in-one configuration management solution can be a benefit for network automation: A good solution can *enforce* a process.

For example, imagine that your network devices are configured with passwords that aren't known to your administrators and engineers. Instead, only your configuration management solution "knows" the passwords (perhaps written copies are kept in a fire safe as a form of insurance). Thus, administrators *can't* exercise poor practices by directly configuring devices; they're *required* to go through the configuration management solution because only it has the passwords needed to implement changes. Thus, your entire process is *enforced*, ensuring that appropriate change reviews and approvals occur, that any configuration policies you've created are enforced, and that scheduled maintenance windows are properly utilized. Out-of-process changes become difficult, if not impossible, ensuring that your process is able to do its job of protecting the network and, therefore, the business (see Figure 1.2).



**Figure 1.2:** An effective solution can enforce a configuration management process.



Think of how much easier auditing would be if you could prove that all configuration changes took place within your solution (something easy to prove if it's the only thing with the correct passwords to actually make changes on devices) and that the solution was configured to enforce required configuration settings. Auditors would simply need to verify the policies you had set up in the solution and they would be well on their way to finishing the audit.

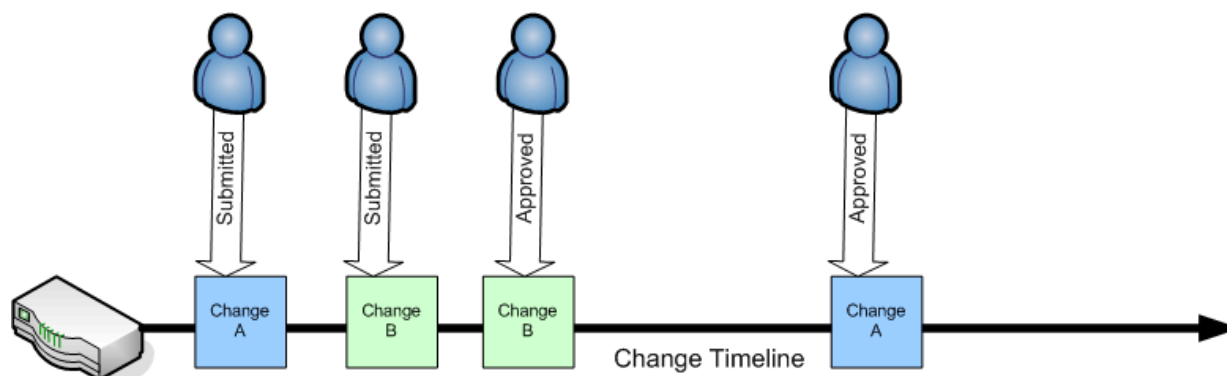
## The Benefits of an Automated Network

Thus far, we've looked at some of the costs of a non-automated network, and some of the challenges and risks that your network must face every day. Let's build on this foundation of knowledge by exploring some of the specific benefits of a fully automated network. Remember, for the most part, these benefits are ones that can *only* be achieved through automation of some kind—you won't really have them if you're running your network manually.

### Configurable

Above all, an automated network is highly *configurable*, meaning it can be changed and reconfigured as quickly as your organization requires, while maintaining a safe, controlled configuration management workflow. Despite the fact that a process of any kind is often viewed as a hindrance, an effective configuration management solution can implement a process almost invisibly. In fact, by providing an application through which the workflow takes place—where changes can be submitted and scheduled, changes can be reviewed and approved, and so forth—the process is often made easier because everything a person needs to participate in the process is readily available.

Configuration management solutions—useful ones, at least—can also help prevent change *conflict*. For example, consider the timeline of changes shown in Figure 1.3.



**Figure 1.3: Timeline of changes to a device.**

This figure illustrates two users who submit changes. Suppose that each change modifies the same portion of the router configuration. Because Change A isn't in effect at the time Change B is developed, Change B is based on the router's current configuration, just as Change A is. Change B is then approved for deployment *before* Change A (perhaps Change B is a higher-priority change). You now have two changes in the queue waiting for deployment, and they're going to conflict with one another. An effective configuration management solution can help resolve this conflict in one of two ways:

- Notify the person submitting Change B that another pending change affects the same area of the device configuration.
- Notify the person submitting or approving Change A that another change (Change B) has been approved that affects the same area of the device configuration.

Particularly in large environments, this sort of conflict resolution can help prevent mistakes and ensure that devices retain a high degree of configurability.

### **Consistent**

Perhaps one of the most important benefits an automated network offers is consistency. When a configuration management solution is used to manage devices, configurations can be designed *once*, entered *once*, approved *once*, then deployed consistently to all appropriate devices. The key is that the manual portion of the process is performed only *once*, reducing the chance for error, and even that one manual step can be reviewed for accuracy.

An effective configuration management solution goes even a step further and helps to eliminate error-prone manual configuration. For example, a solution might allow you to configure a device in a test lab, then, when you've got the configuration working just the way you want, capture that configuration to use as a model for configuring other devices. This process creates a high level of consistency and a very low rate of error, helping to improve the network's overall reliability and security.

Consistency is the key to so much of a well-run network:

- **Security**—When devices are configured consistently, the overall network is more secure because no one device represents a potential weak point due to a poor, inconsistent configuration. For example, if you can imagine an administrator trying to manually deploy even a short access control list (ACL) change similar to the following example, you can also imagine how many errors could creep in:
 

```
access-list 100 remark VTY Access ACL
access-list 100 permit tcp host 7.7.7.5 host 0.0.0.0 range 22 23
log-input
access-list 100 permit tcp host 6.6.6.1 host 0.0.0.0 range 22 23
log-input
access-list 100 deny ip any any log-input
```
- **Manageability**—Consistently configured devices are easier to manage because they all follow the same conventions; administrators don't have to spend as much time examining configurations before proposing new changes because devices can be relied upon to have the same basic configuration.
- **Reliability**—Because devices with consistent configurations use a single, tested configuration, they are less likely to have configuration errors that result in network downtime.

It sounds simple, but consistency is probably the most desirable trait in any network, and an automated network is pretty easy to keep consistently configured.

### **Recoverable**

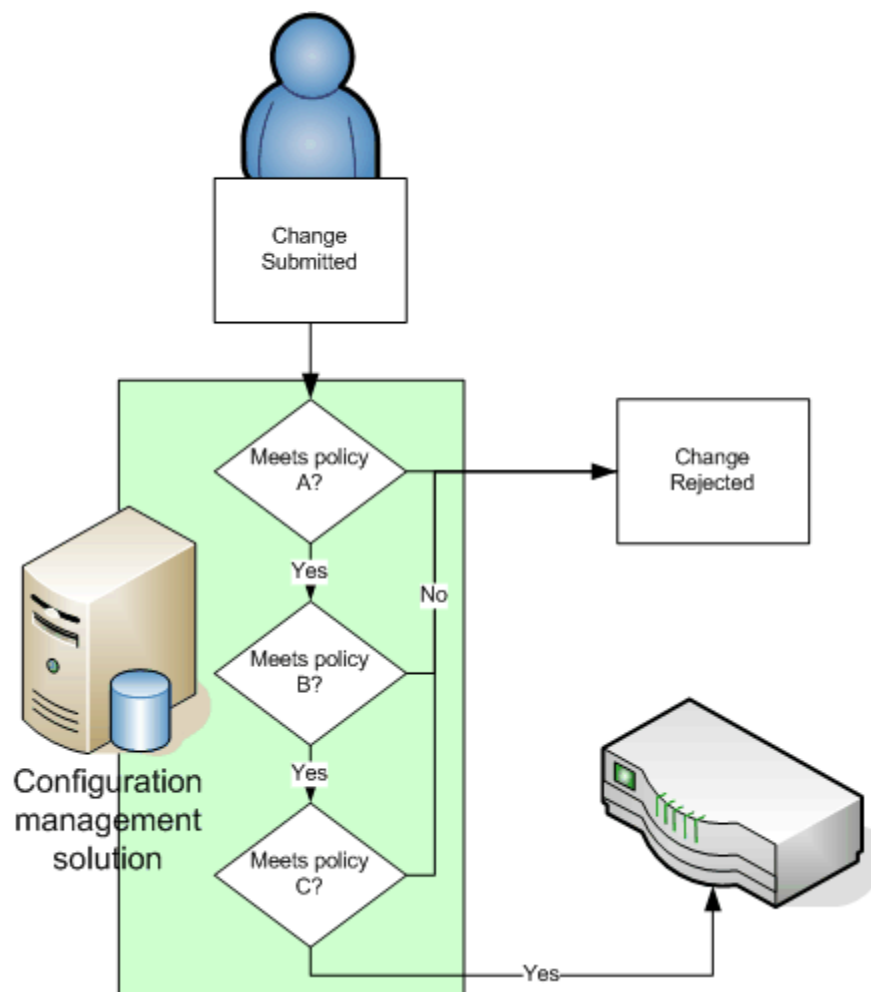
Some disasters are beyond your control to prevent or even anticipate—loss of utility power, natural disasters, and so forth. But even smaller disasters—a failed device, a missed configuration error, and so forth—can result in network downtime. A *recoverable* network can bounce back from these problems quickly, and automation can provide that capability. Because

configuration management solutions can provide a complete configuration repository of *every* past version of *every* device's configuration, a solution can be used to restore any one of those configurations, either to the original device—in the case of a misconfiguration—or to a backup device—in the case of a device failure or natural disaster.

An effective configuration management solution grabs not only periodic scheduled backups of devices' configurations but also point-in-time backups in reaction to a change in the device's configuration. For example, a solution might monitor syslog or TACACS+ accounting traffic, or even SNMP traps, to notice when a device's configuration may have changed (a syslog entry indicating that the device was placed into configuration mode, for example, is a good clue that a change has occurred). The solution can use that cue to grab the device's configuration, essentially providing an automatic backup every time a change occurs, or could have occurred, to a device. You can then roll back that device's configuration to any point in time, which is truly the ultimate in recoverability.

### Securable

A secure network is a goal for most organizations. How does automation improve security? Consistency is one way. Another way is through policy enforcement. Consider Figure 1.4.



*Figure 1.4: Policy-based management.*

Because security-related configuration settings are so important, a configuration management solution can be configured to proactively enforce policies. In other words, in addition to scanning existing device configurations for policy compliance, a solution might also review all submitted changes. Changes that meet all configured policies are cleared for deployment; changes that don't meet all configured policies are rejected before ever making it to a device.

Configuration management solutions can also provide much more granular security than network devices can offer. For example, a configuration management solution might be able to allow entry-level technicians to perform basic operations such as restarting a device, while only more experienced technicians are allowed to submit configuration changes to the device. Auditors might be able to access devices' configurations in a read-only fashion. This role-based security helps to automate and control access to device configurations, also improving the overall security of the network.

### **Compliant**

Security isn't *quite* the same thing as compliance. True, most compliance legislation concerns itself with security, so the two are definitely tightly intertwined, but they're not precisely identical. In a secure network, you've simply got everything configured to be however secure you want it; for a *compliant* network, you have to be able to prove it. In other words, compliance is almost a union between having a secure and auditable network.

Typically, compliance management works like this: You assemble a checklist of configuration parameters that, if implemented, result in your network complying with whatever rules and regulations you're required to comply with—the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act, CISSP, and so forth. Typically, you also need to have a process that prevents unauthorized changes to these critical configuration areas. You must then be able to demonstrate your compliance—prove that the correct configurations are in place, that they *have been in place*, and that, thanks to your process, they're likely to remain in place in the future.

How can network automation help with compliance? In several ways:

- Policy-based management can be used to enforce key configuration parameters, either by automatically alerting you to unauthorized changes or, better yet, automatically remediating unauthorized changes.
- An enforced workflow ensures that unauthorized changes can't occur. If all changes have to go through a configuration management solution, and if that solution enforces a workflow, you will remain in compliance.
- Configuration management solutions that automatically grab backups of device configurations can report on any unauthorized changes. This process “closes the loop” on compliance: With policy-based management and an enforced workflow, unauthorized changes should be impossible; reports based on analysis of actual device configurations proves that unauthorized changes haven't occurred.

## **Auditable**

Any network is auditable. The difference is that an automated network is *easily* and *continuously* auditable. In a manual network, auditing requires that you dump each device's configuration and then manually examine it. As with manual configuration, this process is error-prone. Imagine reading through a 300-line configuration file—you're going to miss a few details; multiply this example by hundreds of devices and the review quickly becomes an almost pointless exercise.

With automation, this process is much easier. An effective configuration management solution, for example, will allow you to define the specific configuration parameters that you *want* to see, then generate an exception report of all device configurations that *don't* meet your requirements. Instant audit. What could take weeks to perform manually can literally be done in seconds, because the configuration management solution doesn't need to connect to the actual network devices; it can simply run the report from its own configuration repository, which contains all the devices' current configurations.

## **Efficient**

Need to roll out a change to 500 devices? Need to change passwords on 1000 devices? Need to deploy a patch to 100 devices? In a manual network, you would need to calculate the time it takes to perform the task once, then multiple that time by the number of devices. The numbers add up fast. In an automated network, however, you perform the task only *once*. The automation solution performs it however many hundreds of other times you might require. The savings in time is truly amazing.

In addition, a configuration management solution can perform the mundane tasks associated with a change but not directly part of it—backing up the device beforehand, backing up the device again after the change is applied, ensuring that configuration policies are not violated by the change, and so forth. A well-automated network can be managed with a fraction of the manpower a manually run network requires, freeing up staff for other projects or helping to reduce staff and outsourcing requirements.

## **Flexible**

Finally, one of the most important—and yet often overlooked—benefits of an automated network is flexibility—the business flexibility offered by frameworks such as IBM OnDemand and Hewlett-Packard Adaptive Enterprise; the ability to quickly reconfigure your business to meet new competitive challenges or business needs. With the ability to quickly reconfigure the network in a secure, compliant, consistent fashion, and with the ability to quickly roll back changes in a moment if required, making changes to the network is no longer a great undertaking. The massive risk formerly associated with making changes to the network is highly mitigated by your automated management capabilities, meaning you can bend, flex, and reconfigure your network in whatever way best suits your current business needs. This ability is a major contribution to the long-term profitability and success of any company.



## Traditional Management vs. Automated Management

To wrap up this chapter, let's take a moment to compare and contrast the three major forms of traditional network management with management in an automated network, highlighting the specific differences and benefits.

### *Ad-Hoc Configuration*

Traditional network device management is almost entirely ad-hoc, meaning that changes are made on a per-device basis whenever changes are needed. This is a poor practice, although in many cases, it is done simply because that is how network devices are designed to be managed. The reason ad-hoc management doesn't work is that it is applied inconsistently. For example, it's a common security practice to configure routers with black hole routes rather than using TCP Intercept. In a Cisco device, you would add text similar to the content that Listing 1.2 shows to the configuration file.

```
ip route 1.0.0.0 255.0.0.0 null0
ip route 2.0.0.0 255.0.0.0 null0
ip route 5.0.0.0 255.0.0.0 null0
ip route 7.0.0.0 255.0.0.0 null0
ip route 10.0.0.0 255.0.0.0 null0
ip route 23.0.0.0 255.0.0.0 null0
ip route 27.0.0.0 255.0.0.0 null0
ip route 31.0.0.0 255.0.0.0 null0
ip route 36.0.0.0 255.0.0.0 null0
ip route 37.0.0.0 255.0.0.0 null0
ip route 39.0.0.0 255.0.0.0 null0
ip route 42.0.0.0 255.0.0.0 null0
ip route 49.0.0.0 255.0.0.0 null0
ip route 50.0.0.0 255.0.0.0 null0
ip route 77.0.0.0 255.0.0.0 null0
ip route 78.0.0.0 255.0.0.0 null0
ip route 79.0.0.0 255.0.0.0 null0
ip route 92.0.0.0 255.0.0.0 null0
ip route 93.0.0.0 255.0.0.0 null0
ip route 94.0.0.0 255.0.0.0 null0
ip route 95.0.0.0 255.0.0.0 null0
ip route 96.0.0.0 255.0.0.0 null0
ip route 97.0.0.0 255.0.0.0 null0
ip route 98.0.0.0 255.0.0.0 null0
ip route 99.0.0.0 255.0.0.0 null0
ip route 100.0.0.0 255.0.0.0 null0
ip route 101.0.0.0 255.0.0.0 null0
ip route 102.0.0.0 255.0.0.0 null0
ip route 103.0.0.0 255.0.0.0 null0
ip route 104.0.0.0 255.0.0.0 null0
ip route 105.0.0.0 255.0.0.0 null0
ip route 106.0.0.0 255.0.0.0 null0
ip route 107.0.0.0 255.0.0.0 null0
ip route 108.0.0.0 255.0.0.0 null0
ip route 109.0.0.0 255.0.0.0 null0
ip route 110.0.0.0 255.0.0.0 null0
ip route 111.0.0.0 255.0.0.0 null0
```

```
ip route 112.0.0.0 255.0.0.0 null0
ip route 113.0.0.0 255.0.0.0 null0
ip route 114.0.0.0 255.0.0.0 null0
ip route 115.0.0.0 255.0.0.0 null0
ip route 116.0.0.0 255.0.0.0 null0
ip route 117.0.0.0 255.0.0.0 null0
ip route 118.0.0.0 255.0.0.0 null0
ip route 119.0.0.0 255.0.0.0 null0
ip route 120.0.0.0 255.0.0.0 null0
ip route 121.0.0.0 255.0.0.0 null0
ip route 122.0.0.0 255.0.0.0 null0
ip route 123.0.0.0 255.0.0.0 null0
ip route 127.0.0.0 255.0.0.0 null0
ip route 169.254.0.0 255.255.0.0 null0
ip route 172.16.0.0 255.240.0.0 null0
ip route 173.0.0.0 255.0.0.0 null0
ip route 174.0.0.0 255.0.0.0 null0
ip route 175.0.0.0 255.0.0.0 null0
ip route 176.0.0.0 255.0.0.0 null0
ip route 177.0.0.0 255.0.0.0 null0
ip route 178.0.0.0 255.0.0.0 null0
ip route 179.0.0.0 255.0.0.0 null0
ip route 180.0.0.0 255.0.0.0 null0
ip route 181.0.0.0 255.0.0.0 null0
ip route 182.0.0.0 255.0.0.0 null0
ip route 183.0.0.0 255.0.0.0 null0
ip route 184.0.0.0 255.0.0.0 null0
ip route 185.0.0.0 255.0.0.0 null0
ip route 186.0.0.0 255.0.0.0 null0
ip route 187.0.0.0 255.0.0.0 null0
ip route 192.0.2.0 255.255.255.0 null0
ip route 192.168.0.0 255.255.0.0 null0
ip route 197.0.0.0 255.0.0.0 null0
ip route 223.0.0.0 255.0.0.0 null0
```

**Listing 1.2:** Example addition to a configuration file.

That is a long list. Although you can add this content to a template, it's easy to enter a mistake when you're configuring devices manually. In an automated network, however, you might use a configuration management solution to make these settings policies. The solution could also have a job that applies these settings, and the policy could be linked to the job for remediation. The solution would then simply scan every appropriate device to make sure these settings are in place, per the policy; if they weren't, the solution would run the job that puts these in place. You would only configure these settings once, and they would be consistently deployed to appropriate devices *automatically*. If these settings ever change, you would simply change your policy and the remediation job; the solution would then take care of reconfiguring devices to match the new policy.

Ad-hoc changes have another problem—a lack of workflow. Although your company may have a configuration management process for the network, that doesn't mean it's used each and every time a change needs to be made. With an automation solution in place, however, that workflow can be *enforced*, improving the network's reliability and accomplishing everything that your workflow was intended to provide.

☞ In organizations that must meet compliance requirements, such as the Sarbanes-Oxley Act, HIPAA, the Graham-Leach-Bliley Act, and so forth, enforcing a configuration management workflow is typically a requirement that helps you remain compliant. If auditors feel that there is a way for your configuration management process to be bypassed, they may not feel you're capable of remaining compliant. Auditors will fail companies simply because there wasn't an *enforceable* workflow in place.

### **Manual Backup and Recovery**

Backup and recovery are two elements of network administration most often performed poorly when done manually. The very act of logging into every device and commanding it to dump its configuration—typically to a Trivial File Transfer Protocol (TFTP) server—is time-consuming and incredibly inefficient. If you have 800 devices, and it takes you just 3 minutes to back up each one, you're looking at a full 40 hours to get them all. How often are you really going to do that? Plus you're forced to manually manage a configuration repository, ensuring that past backups are kept. If you change a device's configuration, you have to remember to create a new backup—will you always do that when you're in a hurry?

Backup and recovery are often the first two things organizations automate when it comes to network device management. Numerous inexpensive solutions exist for automating basic backup and recovery; these solutions can usually be configured to automatically take a new backup on a scheduled basis and to maintain a repository of configuration backups. Of course, this step is only one tiny part of a fully automated network; all-in-one configuration management solutions provide this automation functionality along with much, much more.

Automated *recovery* is something else. This functionality isn't typically provided by low-end automated backup solutions; instead, automated recovery is usually provided as a configuration management feature. Essentially, a configuration management solution is used to detect changes to devices—often by monitoring SNMP traps or syslog output—and to automatically roll back the device's configuration (in other words, restore the configuration) to the last-known-good version when unauthorized or inappropriate changes are detected. This option is a powerful security feature. If, for example, an administrator or attacker modifies a device directly, the solution can put back the device to its authorized, configuration-managed version automatically.

## Scripted Administration

Scripts are the first tool most administrators turn to for basic automation needs. For example, at <http://forums.vandyke.com/showthread.php?t=370>, you'll find a script designed to automate the backup of device configuration files. This example is a fairly complex script capable of handling different types of devices, including Cisco IOS, CatOS, and PIX devices.

Administrative scripts are a huge part of network device management, and, in fact, most high-end configuration management solutions incorporate scripting to some degree, often generating scripts based on activity so that changes can be deployed consistently to multiple devices. However, manually created and managed scripts—although they offer a basic degree of automation—come at a high price. Because network administrators aren't often trained software developers, their scripts are often difficult for someone else to use and maintain, thus creating a dependency on the person who wrote the script—a problem if that person leaves the company, goes on vacation, or moves on to other duties. As a form of administrative automation, scripts *work*, but they often don't work as well—depending, of course, on who wrote the script—as a professionally designed solution.

## Summary

This chapter has focused on the benefits of an automated network as well as the specific costs your business is facing by *not* using automation in your network operations. It also looked at some of the challenges your network faces, and discussed the ways in which automation can help to mitigate or remove those risks. The next chapter will jump right into how automation works on a more technical level, and how automation can improve your network's security and compliance position.

## Content Central

[Content Central](#) is your complete source for IT learning. Whether you need the most current information for managing your Windows enterprise, implementing security measures on your network, learning about new development tools for Windows and Linux, or deploying new enterprise software solutions, [Content Central](#) offers the latest instruction on the topics that are most important to the IT professional. Browse our extensive collection of eBooks and video guides and start building your own personal IT library today!

## Download Additional eBooks!

If you found this eBook to be informative, then please visit Content Central and download other eBooks on this topic. If you are not already a registered user of Content Central, please take a moment to register in order to gain free access to other great IT eBooks and video guides. Please visit: <http://www.realtimepublishers.com/contentcentral/>.