



realtimepublishers.comtm

Tips and Tricks *Guidetm To*

Network Configuration Management

2005 Edition

AlterPoint

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 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, give feedback on our Web site at <http://www.realtimepublishers.com>, or call us at 800-509-0532.

Thanks for reading, and enjoy!

Sean Daily
Founder & CTO
Realtimepublishers.com, Inc.

Note to Reader: This book presents tips and tricks for seven network configuration management topics. For ease of use, the questions and their solutions are divided into topics, and each question is numbered based on the topic, including

- Topic 1: Configuration Management Best Practices
- Topic 2: Network Management Security
- Topic 3: Network Configuration Troubleshooting
- Topic 4: Change Configuration Management Technologies
- Topic 5: Selecting and Deploying a Network Configuration Management Solution
- Topic 6: Enterprise Network Configuration Management
- Topic 7: Compliance Management for the Network

Introduction to Realtimerepublishers	i
Topic 1: Configuration Management Best Practices	1
Q 1.1: How can we ensure that our configuration management continues to meet best practices? 1	
Q 1.2: What is configuration change management, and why should I care?	2
Q 1.3: What is the best way to “do” configuration change management with network devices? ...	3
Planning for Change	3
Identify Risks	4
Categorize Risks	5
Mitigate Risks	6
Prioritize Changes	8
Managing Changes	8
Want to Know More?	9
Topic 2: Network Configuration Management Security	10
Q 2.1: How does network management contribute to an overall information security plan?	10
Q 2.2: We manage network devices by using Simple Network Management Protocol. Are there security risks?	11
Topic 3: Network Configuration Management Troubleshooting	14
Q 3.1: We are having difficulty determining who made changes to network devices when configuration troubles occur. What can we do?	14
Q 3.2: What is the first step toward fixing a router that isn’t working?	16
Topic 4: Configuration Change Management Techniques	18
Q 4.1: Which new technologies can help ease network configuration management?	18
Q 4.2: How can I back up all of my network devices?	20

Topic 5: Selecting and Deploying a Network Configuration Management Solution	22
Q 5.1: How do network configuration management solutions support policy-based management?22	
Topic 6: Enterprise Network Configuration Management	26
Q 6.1: How does policy-based management make it easier to manage a large numbers of devices?.....	26
Topic 7: Compliance Management for the Network	31
Q 7.1: How can policies help us better manage regulatory compliance for our network?	31
Q 7.2: What does my network configuration have to do with compliance?.....	32

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.

Topic 1: Configuration Management Best Practices

Q 1.1: How can we ensure that our configuration management continues to meet best practices?

A: The easiest way to be sure that your configuration management meets best practices is to have a tool or a set of tools that help enforce whatever business processes you have identified as being “best practices.” For example, many organizations implement workflow processes for configuration management. Figure 1.1 shows a simplified management process that could benefit—as the callouts highlight—from solutions to help enforce the workflow.

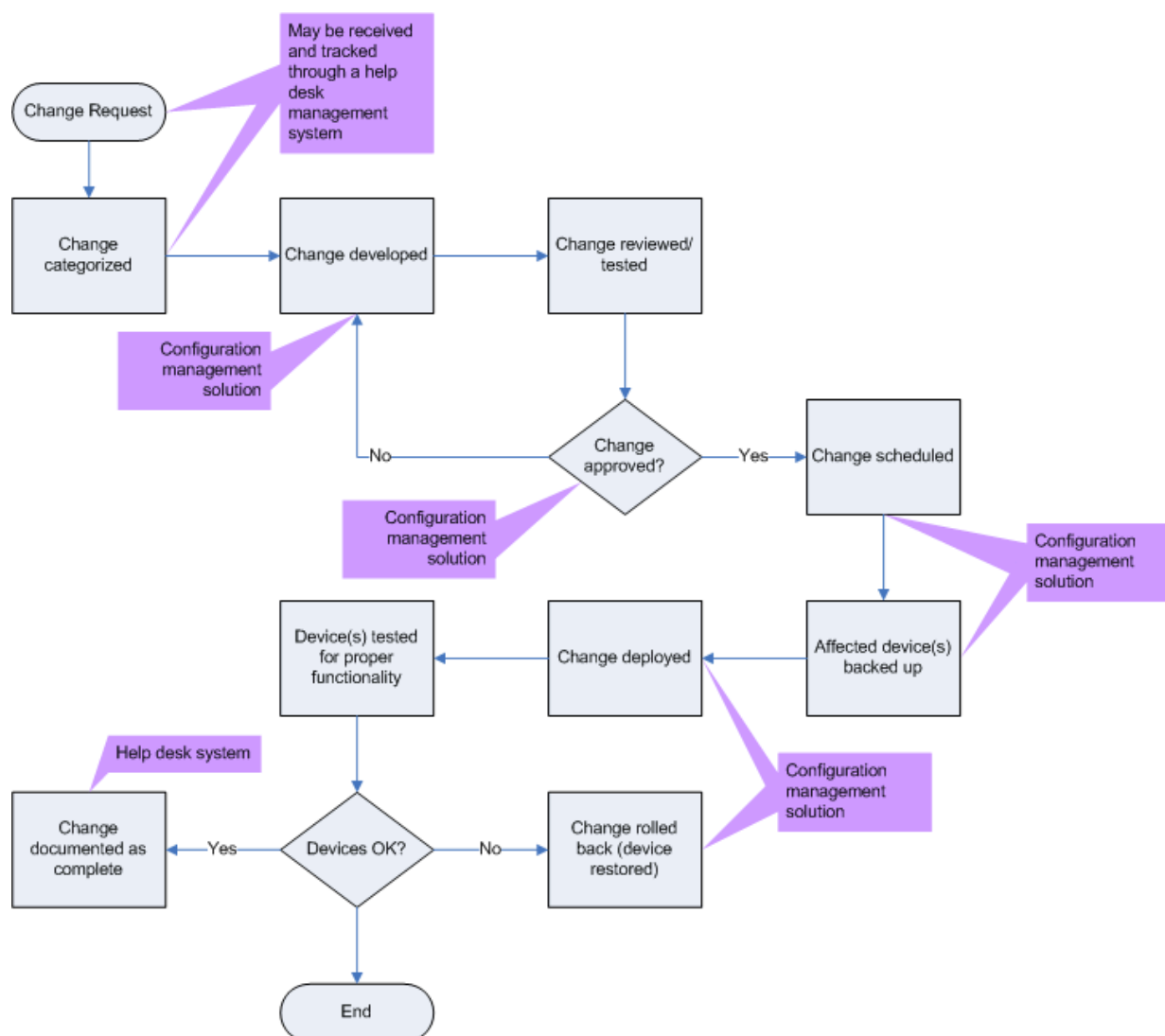


Figure 1.1: Simplified configuration management process.

This process includes workflow steps for receiving and categorizing changes (by risk, priority, and so on); a process that can generally be assisted within a Help desk management system. The change is then developed and reviewed—an important step that can be enforced by a network configuration management solution that includes customizable workflow capabilities.

Essentially, the solution becomes the only interface through which changes are introduced into the network, and the solution itself implements its own level of security to ensure that only approved individuals can enter changes into the system, and that only authorized individuals can review and approve those changes for a production deployment. The solution can also automatically schedule the change for deployment; that deployment can include an automated backup of targeted devices' existing configurations. Those backups can be used to roll back the change if the change does not function as expected or causes a problem.

It is always possible for an administrator to modify a device's configuration directly, bypassing the solution you have implemented and the workflow that it enforces. One way to help prevent such activity is to ensure that your network devices are configured to log activity to a syslog server or a Remote Authentication Dial-In User Service (RADIUS)/Terminal Access Controller Access Control System (TACACS) accounting server or to send SNMP traps. All of these forms of logging can be intercepted by a network configuration management solution, triggering the solution to query the device's configuration via Trivial File Transfer Protocol (TFTP) or by other means. The solution can then compare the device's configuration with the device's last approved configuration, and if any differences are discovered, roll back the device configuration or, at the very least, notify a manager of the discrepancy. This scenario doesn't *prevent* out-of-process changes from occurring, but it can help detect them quickly and remediate them, if necessary, returning devices to their known-good configuration state.

Q 1.2: What is configuration change management, and why should I care?

A: No matter how large or small your network environment, change is inevitable. Hiring new employees, adding new offices, supporting new network services, improving security, fixing bugs—all of these activities result in change, especially to your network infrastructure devices, such as routers, switches, hubs, firewalls, and so forth. Although change is almost always a good thing in the end, change can cause bad things to happen. For example, a careless typo in a firewall configuration file could have alarming security implications. So no matter how minor or beneficial a change may be, you should always approach change with a healthy dose of caution. *Configuration change management* is a set of policies and procedures that you adopt and follow to formalize that caution into a repeatable, consistent process.

At its simplest, configuration change management simply means keeping track of the changes you make and evaluating proposed changes for their effect before actually implementing them. In practice, change management involves some fairly well-defined tasks:

- Maintaining documentation that describes the current configuration of all network devices
- Maintaining documentation that describes the purpose and details of any changes
- Maintaining an archive of older configurations so that they can be used in an emergency
- Implementing policies that control the rate of change
- Implementing policies that control who may perform changes

Why should you bother with all of that? Primarily, to improve network uptime. Unauthorized or unplanned changes are the number one cause of network device failures and unplanned downtime for organizations. Failure to document current configurations makes it difficult, if not impossible, to recover gracefully from a failed change procedure. Failure to control the rate of change as well as who can make changes results in an inconsistent environment that is difficult to maintain long-term. Unauthorized changes can also result in the network no longer complying with regulations or legislation that might apply to your organization, such as the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act, the Graham-Leach-Bliley Act, and so forth. Changes that take your network out of compliance can result in hefty fines, government penalties, loss of customers, and so forth.

Instead of thinking of change management as extra work, consider change management a measure that *saves* your organization work: By simply following some simple methodologies and processes, you can ensure that changes to network devices never become a nightmare. Or, at least, if they *do* become a nightmare, you can quickly recover without having to spend all night at the office!

Q 1.3: What is the best way to “do” configuration change management with network devices?

A: The actual mechanics of change management depend on which types of devices and tools you have on your network; the ways in which you should conduct a change management program, however, are universal. There are two main steps to a change management program: planning and management.

Planning for Change

Too many change management methodologies ignore the planning phase, which is perhaps the most important. Planning allows you to identify and reduce risk, provide a means to rollback in case of disaster, and so forth. Essentially, planning requires you to

- Identify everything that could possibly go wrong as a result of a change.
- Assign a level of likelihood and severity to each potential risk.
- Identify means of mitigating risks or, at least, provide a means of recovery should the risk actually become a reality.

A solid change management planning methodology will make it easier for you to prioritize changes according to their business impact. For example, if you find yourself making several high-risk, low-benefit changes, you can implement policies to reduce such activity, for example, by adopting a policy of only making low-benefit changes during a regular update cycle, such as at the end of each month.

How you actually conduct each step of the planning process depends on your environment and your personal preferences. The next four sections provide some examples to get you started.

Identify Risks

What might go wrong when you update the routing table on one of your routers? Many possibilities spring to mind:

- You could mistype something and corrupt the entire routing table, making the router functionally useless.
- You could enter incorrect information, preventing the change from working properly.
- You could enter incorrect information that makes existing routes stop working correctly.
- While uploading changes to a router, you could lose your network connection, resulting in a partial change to the router.
- You could upload changes to the wrong router, causing routing problems across the network.
- Any incorrect changes you make could replicate across your network through routing protocols, corrupting all of your network devices.

The objective with your risk list is to identify everything that could *possibly* go wrong, not just the things that are *likely* to go wrong. Keep in mind that changing the configuration of *any* network device, not just a router, creates a set of potential risks.

👉 Keep your risk lists handy! After you've developed a list of risks for a particular type of change, such as a router update or a firewall change, keep that list. You are likely to make the same type of change again in the future, so there is no reason to unnecessarily repeat the risk-identification process. You will be building your risk list into a checklist for *avoiding* risks, so the list can become part of your network's change management documentation and act as a list of procedures to be followed to help avoid unnecessary risk during network device management.

Categorize Risks

After you've got a list of everything that could go wrong, assign likelihood and a severity to each item. I prefer a simple scale of 1 to 3, where 1 represents highly unlikely risks, or risks that would be very minor if they did occur, and 3 represents risks that are likely to occur and would be very severe if they did. Working with the previously created list of potential risks, you might assign the following ratings:

- You could mistype something and corrupt the entire routing table, making the router functionally useless—likelihood is 2, severity is 3. The likelihood is high because you manually type all the router configuration information and, although you're always careful, there is no data-validation process in place.
- You could enter incorrect information, preventing the change from working properly—likelihood is 2, severity is 1. Severity is less than that of the first risk because you're simply failing to implement the change, not affecting anything else.
- You could enter incorrect information that makes existing routes stop working correctly—likelihood is 2, severity is 2. The severity is 2 for this risk because you're affecting an entire device.
- While uploading changes to the router, you could lose your network connection, resulting in a partial change to the router—likelihood is 1 because you have backup power supplies everywhere and a very reliable network; severity is 2 because if the risk did occur, it would take the entire device offline.
- You could upload changes to the wrong router, causing routing problems across the network—likelihood is 1 because you are careful; severity is 2 because if you did make this blunder, you would ruin an entire router.
- Any incorrect changes you make could replicate across your network through routing protocols, corrupting all your network devices—likelihood is 3 because if you do make an incorrect change, it will propagate fairly rapidly; severity of 3 because this mistake could potentially take your entire network offline.

The purpose of this list is to help identify the risks that are in most need of specific mitigation. The risk list for a switch reconfiguration might include similar items, but the risks listed would be unique to switches; the same can be said of firewalls, managed hubs, or any other network device. One simple way to rank your risks is to add your two ratings, giving you a prioritized list of things that could go wrong:

- Any incorrect changes you make could replicate across your network through routing protocols, corrupting all of your network devices—risk: 6.
- You could mistype something and corrupt the entire routing table, making the router functionally useless—risk: 5
- You could enter incorrect information that makes existing routes stop working correctly—risk: 4
- You could enter incorrect information, preventing the change from working properly—risk: 3

- While uploading changes to the router, you could lose your network connection, resulting in a partial change to the router—risk: 3
- You could upload changes to the wrong router, causing routing problems across the network—risk: 3

With this list in hand, you are ready to start planning ways to avoid these risks and, should the worst happen, recover as quickly as possible. Again, although I'm using a router in this example, you will want to prioritize the risks associated with changing any type of network device.

Mitigate Risks

Risk mitigation is a planning process in which you try to think of ways to prevent your identified risks from ever occurring; while at the same time coming up with a means of recovery should the risk become a reality in spite of your efforts. Add the mitigation and recovery ideas to your list to create a risk-avoidance and recovery checklist:

- Any incorrect changes you make could replicate across your network through routing protocols, corrupting all your network devices.
- Avoidance—Disable routing protocols on router until change is verified by a senior administrator.
- Recovery—Ensure that a backup of all router configurations is available before you make a change. In the event that incorrect data propagates, immediately restore device configurations from backup.
- You could mistype something and corrupt the entire routing table, making the router functionally useless.
- Avoidance—Use vendor-supplied tools to make changes rather than manually entering changes. Vendor tools provide some data validation to help prevent data-entry errors. Also, document all changes and have another administrator review and approve them for accuracy. Have the other administrator verify the accuracy of the changes after they are made.
- Recovery—Back up the device configuration before making a change. Immediately restore the device configuration if changes made do not comply with the change documentation.
- You could enter incorrect information that makes existing routes stop working correctly or prevents the change from working properly.

Avoidance—Use vendor-supplied tools to make changes rather than entering changes directly in router. Vendor tools provide some data validation to help prevent data entry errors. Also, document all changes on paper and have another administrator review and approve them for accuracy. Have the other administrator verify the accuracy of the changes after they are made.

Recovery—Back up the device configuration before making a change. Immediately restore device configuration if changes made do not comply with the change documentation. Always have a workstation available that can make a direct serial connection to the router in case an incorrect change disables the router's ability to communicate via network interface.

- While uploading changes to the router, you could lose your network connection, resulting in a partial change to the router.

Avoidance—Ensure that router, administrative workstation, and intermediate devices (hubs and switches) are on power backup. If possible, place an administrative workstation on same network segment as the router to be changed to eliminate the possibility of an intermediate router failure during upload.

Recovery—Back up the device configuration before making a change. Ensure that the router being changed is accessible to a local-segment workstation on which the back up resides, allowing easier restore. Always have a workstation available that can make a direct serial connection to the router in case an incorrect change disables the router's ability to communicate via network interface. As a last-ditch recovery method, many network devices offer a hardware reset switch that restores the device's factory configuration. Combined with a recent configuration backup, you can use this reset function to quickly get the device up and running again.

- You could upload changes to the wrong router, causing routing problems across the network.

Avoidance—Have another administrator confirm your changes and settings prior to upload.

Recovery—Back up all network devices before making a change. If data is uploaded to the wrong device, restore that device's configuration from backup. Always have a workstation available that can make a direct serial connection to the router in case an incorrect change disables the router's ability to communicate via network interface.

Some network devices, such as managed hubs and switches, might offer simpler recovery methods. Some managed hubs, for example, can create a backup of the last-known good configuration to a built-in flash RAM module, and let you recover that configuration with a hardware reset switch. Other network devices, such as firewalls, might require more extensive planning to ensure that a fast recovery is possible.

👉 After you have developed a complete risk list, including mitigations, for a particular type of change, save it! This list should become a checklist for all future changes of the same type. By following the checklist each time you make that type of change, you will automatically mitigate the potential risks as well as have prepared recovery options in case the worst happens. If your network administration is primarily accomplished by junior administrators, these mitigation lists can become a mandatory part of the procedures the administrators follow, helping ensure that you're sort of looking over their shoulder, even when you're not.

Prioritize Changes

Don't get into the habit of making every change that pops into your head. Prioritize changes based on their impact on business operations. You can use a simple 1-to-3 scale or something more complex. High-priority changes are worth more risk, of course, while lower-priority changes—especially those with a high-risk rating—should be put off until they can be made under tightly controlled circumstances. For example, some companies save all low-priority changes until the end of the month. Before implementing any changes, they carefully review them all. They also back up every single network device in case something goes horribly wrong, and they put the necessary support personnel on alert. This process requires a lot of effort and isn't something that these companies want to go through on a daily basis.

☞ Software tools can make this process easier, of course, by automatically backing up devices prior to deploying a change, and by automatically deploying changes for you on a schedule you set.

For emergency changes that need to be implemented immediately, the companies have a fast-track process that requires two senior administrators to approve and implement the change; the idea being that senior administrators have enough experience to pull off the change with less risk. How you prioritize and handle changes really becomes a matter of change management policy, which I'll discuss next.

Managing Changes

Changes can easily get out of control, and the only way to rein them in is to have in place a firm set of change management policies that all administrators are required to follow. For example, you might implement a change management policy as follows:

- All changes must be documented and approved by a senior administrator. Change documentation must include the current state of the device as well as the proposed change.
- Changes identified as high-priority require a senior administrator's approval. All other changes require the approval of two administrators, including at least one senior administrator.
- All changes must include a detailed description of the intent of the change (for example, To allow the Nevada office to communicate directly with the Seattle office rather than communicating through the New York hub office).
- All completed changes will be reviewed at a weekly meeting of administrators. This meeting will help make all staff aware of recent changes and allow an opportunity to review failed changes.
- Changes classified as emergency priority can be made only by two senior administrators working together. These changes can bypass the normal review process, but that process will be completed as soon as possible after the change is complete to ensure that a complete set of documentation for the change is created.

The actual policies your company might adopt may differ; however, the important point is to have some procedural guidelines in place.

☞ You can use software tools to help enforce a change management methodology. For example, some tools let changes be developed and deployed to test devices but require a second administrator or manager to review and approve changes before they can be deployed to your production devices.

Want to Know More?

No matter what you do, make sure that you have a system in place for change management. If you would like some ideas for how to physically implement such a system, check out the University of Kentucky's Change Control FAQ, located online at <http://www.uky.edu/~change/faq.html>. This site should give you some ideas of how a change management system works at a very high level, including change requests, tracking, and so forth. You should also check out Cisco System's excellent white paper about change management, available at <http://www.cisco.com/warp/public/126/chmngmt.shtml>. This white paper provides a great overview of change management and gives detailed examples of process flows. The white paper also provides examples of change management documentation, which can help jump-start a new change management process in your organization. Another great resource is the Information Technology Infrastructure Library (ITIL) at <http://www.ogc.gov.uk/index.asp?id=2261>, which provides several best-practices frameworks for IT management, including change management.

Topic 2: Network Configuration Management Security

Q 2.1: How does network management contribute to an overall information security plan?

A: Many companies have detailed information security plans, including physical security of information, electronic security, and more. They implement technologies such as IPSec to encrypt sensitive information and 802.1X to help restrict who can connect to the network, and they use detailed firewall configurations to help ensure that only authorized traffic crosses from the internal network to the Internet. These companies have almost no security whatsoever on their network devices—the same devices that ensure that IPSec functions, 802.1X is properly configured, the firewalls remain properly configured, and so forth. Some of these companies even have their devices' read-write SNMP community strings set to "private," making those configurations anything *but* private for anyone managing to get into the device's configuration.

Any security plan is, of course, only as good as its weakest link, and in the case of these organizations, the network devices are the weakest link. Because the devices are so poorly secured and implement core security technologies, the entire network becomes more susceptible to attack than it need be. In addition to security concerns, these companies can face major regulatory compliance requirement problems that result from the lack of security at the network device layer.

The problem most of these companies have is not a lack of understanding about security or networking technologies; they simply have poor policies regarding network management and don't understand the impact that unsecured network devices can have on their carefully thought out security plan. One reason behind their problem is that they have given high-level business policies to their network administrators. For example, a policy such as *Only authorized computers must be able to connect to the network and obtain a DHCP address* tells a network administrator that 802.1X might be called for; it doesn't, however, say anything about securing the network switches that actually implement 802.1X. These companies need to specify some additional policies regarding the security of network devices.

When working with network policies, start with the high-level business policies, which are generally driven by specific business requirements. From there, develop technological policies, which are implemented by specific technological rules. This method creates a one-to-one mapping that both business and technology professionals can understand more easily. Figure 2.1 illustrates the concept.

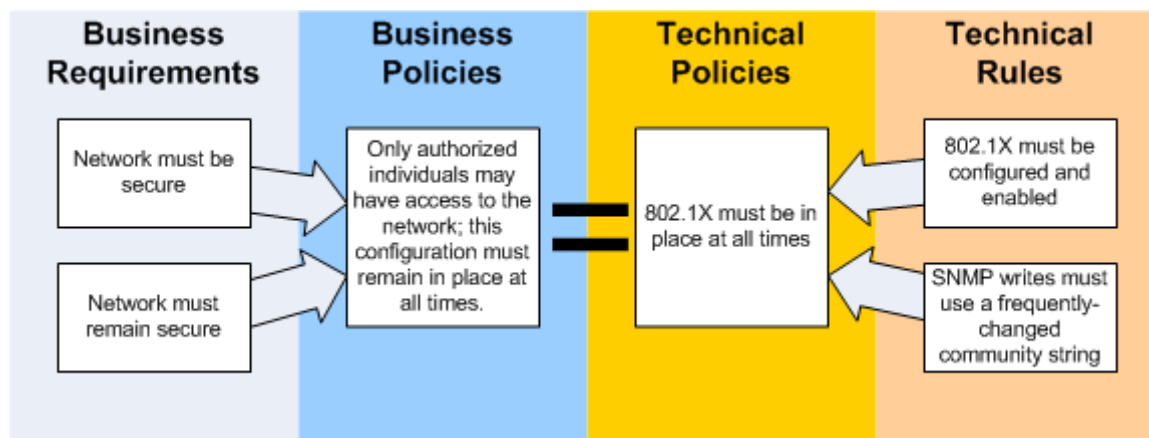


Figure 2.1: Mapping business requirements and policies to technical policies and rules.

Once you have defined policies and rules at this level, you can begin implementing them on network devices. Actually taking the time to write out your policies—and how they relate to one another—has two beneficial effects:

- You will be communicating policies and requirements more clearly and effectively
- You will be able to more easily spot any gaps in your policies and rewrite them or draft additional policies to fill the holes

Finally, a new generation of network configuration management solutions is able to manage your devices directly from these policies, rather than simply managing raw device configurations. This policy-based management is a key driver behind so-called agile business strategies such as Hewlett-Packard (HP) Adaptive Enterprise, IBM OnDemand, and Microsoft Dynamic Systems Initiative.

Q 2.2: We manage network devices by using Simple Network Management Protocol. Are there security risks?

A: You betcha. For starters, remember that Simple Network Management Protocol (SNMP) can be used to read and write (*set*) information on network devices. Reading might not seem like a security risk, but it is. Attackers can use the information gleaned from SNMP to learn more about your network's infrastructure, effectively building a complete blueprint of your network. Every movie that includes bank break-ins teaches us that a blueprint is the best way to plan your attack, so denying attackers your network blueprint is a wonderful first defense. Of course, SNMP's ability to change network devices' configuration settings can, of course, be lethal. The following list highlights tips for keeping SNMP from becoming a hazard:

- Disable SNMP entirely, if you can. Other, more secure, management protocols are available (most of them proprietary, such as Hewlett-Packard's Insight protocol). At the very least, configure your devices for read-only SNMP, and make configuration changes through other means, if possible.
- If you are not using SNMP, you definitely need to disable it in your devices. You might think that your firewall prevents Internet intruders from using SNMP to attack your devices, but don't forget about internal intruders or just plain mischievous users!

- Change your SNMP community strings often. Once a week isn't too often. Of course, changing strings on all your devices can be a tedious task, so check whether your network device vendors offer any tools to automate the process. Again, don't assume that your devices are safe from attack just because they are behind a firewall!



Never ever leave your SNMP community strings set to "public," which is often the default setting. Every attacker knows to try that first.

- The SNMP specification requires community strings to be case-sensitive, so use a mix of uppercase and lowercase letters as well as numbers. In addition, don't use cutesy community strings; use completely random ones, just as you would for an especially secure password. For example, e3N7Rft8eH8H would make an effective community string.
- Configure boundary devices, such as firewalls, to block SNMP traffic from entering or leaving your network.
- Ideally, build a separate network to carry SNMP traffic, and physically separate it from your production network. This technique will make it more difficult for hackers to get SNMP traffic to your devices. And never forget that hackers can come from within; simply blocking SNMP at the firewall isn't sufficient to protect your devices. A separate network will also help protect against SNMP Denial of Service (DoS) attacks (when an attacker fires invalid SNMP packets at devices in an attempt to bog them down and prevent them from responding to legitimate requests). A separate network is definitely an expensive proposition; however, it provides the ultimate in security for your network devices. Organizations that have especially stringent security requirements, such as banks and government-regulated entities, might find the investment worthwhile.
- Higher-end devices can often be configured to accept SNMP instructions only from a specific IP address or address range. Determine whether your devices support this capability, and if they do, use it. Set up your administrative workstations and management consoles with fixed IP addresses (either static IP addresses or Dynamic Host Configuration Protocol—DHCP—reservations) and instruct your devices to ignore SNMP instructions that come from any other IP address.
- Stay up to date on your device's operating system (OS) updates. Most network device manufacturers release regular patches and security bulletins to help make their devices as secure as possible. Many manufacturers provide electronic mailing lists to which you can subscribe; use those lists to notify you of the latest fixes. Patches should, of course, fall under a configuration management procedure to help ensure that they are properly deployed and that they create a minimal impact on production.
- Log SNMP traffic. Some devices provide an option to automatically log received SNMP requests. If they don't, you can use a network sniffer device to monitor SNMP traffic and capture any that it sees passing on your network. Even if you only run the monitoring software occasionally, it will help detect any unauthorized SNMP traffic on your network.

SNMP can be useful, if you're aware of the risks and take the necessary steps to make SNMP more secure.

A relatively new concept in change management is called *policy-based management*. This management concept generally requires sophisticated tools in order to implement effectively, but the concept is simple: Rather than configuring devices, you configure a set of rules and policies. For example, one rule might simply require devices to have a particular SNMP community string. The rule is then applied to the appropriate devices. The solution analyzes the devices' current configurations and compares them with the rule; devices that do not meet the rule are, at least, flagged for your attention. Better software solutions can automatically correct or *remediate* the problem by *applying* the rule and actually changing the device's configuration to comply. Want to change the SNMP community string on every device? Simple—change the rule. The solution will detect all devices as out-of-compliance and fix them for you (provided it has that capability and you have configured it to do so).

Topic 3: Network Configuration Management Troubleshooting

Q 3.1: We are having difficulty determining who made changes to network devices when configuration troubles occur. What can we do?

A: Auditing is the key to determining who made network device changes. If your organization is dealing with regulatory compliance requirements, auditing is absolutely necessary. However, most network devices aren't terribly well-designed when it comes to auditing. In a robust operating system (OS) such as Microsoft Windows, for example, nearly every type of user activity can be audited—for example, access to files (whether allowed or denied), access to directory objects, and so forth. Details about each activity (which file was accessed, for example) is readily available. Network devices, in contrast, provide much less granularity for their logging and offer much less detail in the logging they provide.

The first step to auditing is to implement a logging system. Most devices can work with Remote Authentication Dial-In User Service (RADIUS), Terminal Access Controller Access Control System (TACACS), Simple Network Management Protocol (SNMP), or syslog for logging purposes. As Figure 3.1 shows, you might implement RADIUS for device authentication and syslog for logging (although you could as easily use RADIUS for both).

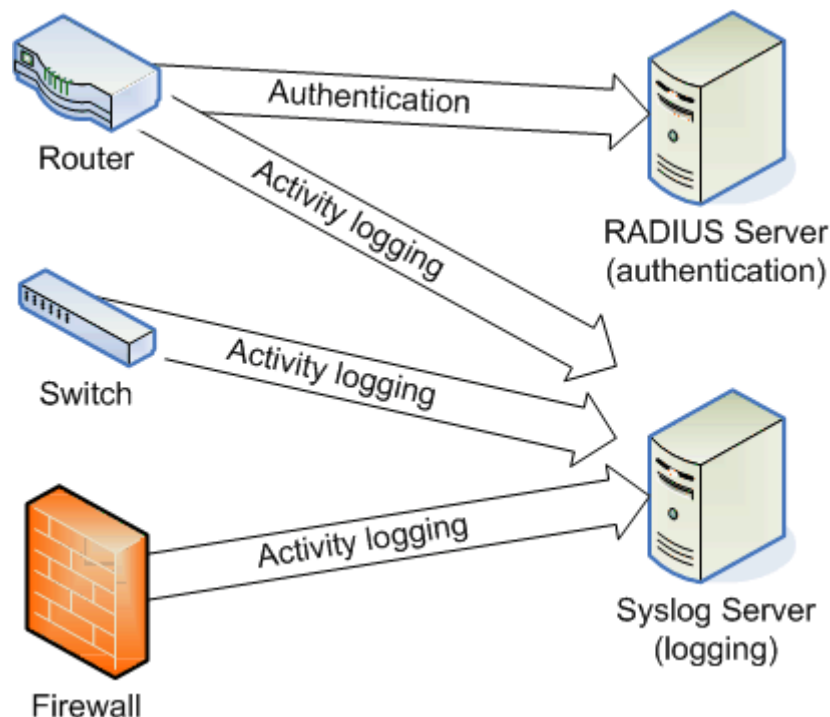


Figure 3.1: Using different technologies for logging and authentication.

Centralized authentication—as provided by RADIUS and TACACS—is crucial to obtaining more insight and control in your network devices. Because administrators are able to use a single, centralized set of credentials to manage all devices, your audit logs will be more consistent and any activity will be easier to relate to a single individual.

The problem with network device logging is that it is not detailed. For example, a network device can generate a log message whenever an administrator enters or exits the device's configuration mode. However, there is no guarantee that the administrator *did* anything in that mode, and there is no telling *what* the administrator did, if anything. In this area, network devices tend to fall short in the auditing department—they lack the detail you need to associate specific changes with a specific individual.

Third-party network configuration management tools can intercept RADIUS, TACACS, SNMP, and syslog traffic, looking for clues that someone might be configuring the devices. Some solutions even go one step further and query the device's configuration, then compare that configuration with an earlier configuration backup. This comparison allows the solution to determine that a change has occurred, what the change involved, and which administrator made the change. This information is useful for both management and troubleshooting purposes, and it fulfills the auditing requirements set down by many pieces of legislation (such as the Health Insurance Portability and Accountability Act—HIPAA, the Sarbanes-Oxley Act, and so forth). Figure 3.2 illustrates the process and shows how the device's normally insufficient logging can serve as a trigger for a more robust auditing plan.

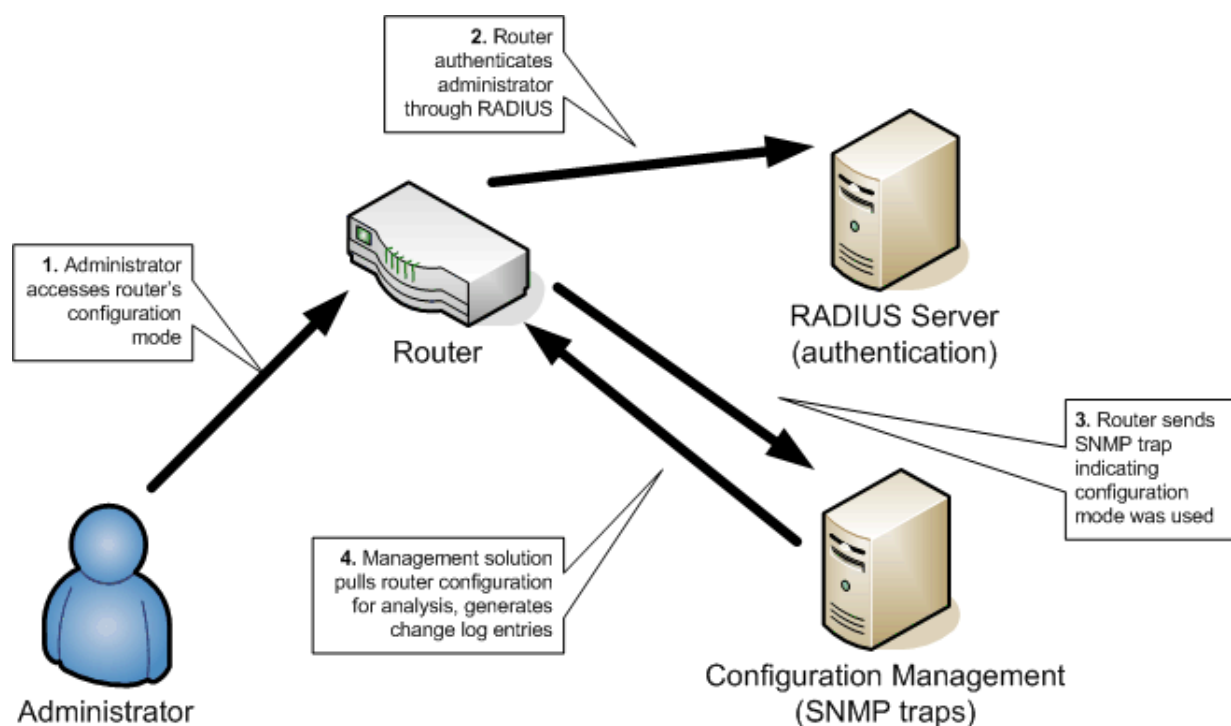


Figure 3.2: Creating more detailed logs by using a configuration management solution.

Network configuration management solutions with these capabilities often store their data in independent databases, allowing the auditing data to be secured and/or encrypted, and allowing more robust reporting. In fact, many solutions include several built-in reports to help highlight recent changes, track changes over time, provide a summary of changes to a particular device, and so forth. Thus, although devices themselves aren't capable of generating extremely detailed who-what-when-where auditing logs, when used in conjunction with a network configuration management solution, you can still get all the auditing information you need to more effectively manage and troubleshoot your network.

Q 3.2: What is the first step toward fixing a router that isn't working?

A: The first question you should ask is “What changed?” Very few network devices go belly up on their own; you'll find that it usually requires human involvement to really screw things up. Assuming that you have eliminated hardware failure as the cause of the problem, the culprit is most likely a recent change made to the device's configuration. Of course, if the hardware is at fault, you simply need to replace the hardware and restore your configuration from a backup.

Restoring from a backup—you do *have* a backup of the router's configuration, don't you?—is a good first step even if the hardware is fine. Ideally, the backup configuration will resolve the problem, and you can use a tool to compare the old and new configurations to determine the differences. This process is not exactly troubleshooting the problem, but unless you're working in a lab, your goal should be to restore the device to operation *first* and determine what caused the problem later.


☞ One change at a time, please! The idea of using a known-good backup to recover from a device failure only works if you tend to make a small number of changes at a time, let them settle to ensure that they're working properly, then immediately make a backup. If you are in the habit of making a raft of changes at once, you will have a much more difficult time tracking down the change that caused the problem.

If you plan to release changes in batches—doing so is a best practice from the ITIL framework—you can only do so if the individual changes *and* the batch have been thoroughly tested to ensure that they won't cause a problem. Obviously, testing is far preferable to the “deploy it to production and see what happens” network management technique.

If you don't actually have a recent backup, shame on you! Hopefully you have change management documentation that describes the changes that have been made to the router in recent memory. Start examining those changes to determine which ones might apply to the problem you are having. If necessary, manually undo each change, one at a time, until the problem is resolved.

Other changes might involve a device operating system (OS) upgrade or patch. In such cases, you should never make a change without understanding how you can roll back to the prior (working) version of the OS. If necessary, keep a spare router on hand in case the OS upgrade or patch kills your production unit. The goal, in any event, is to not worry so much about troubleshooting the current problem, and to simply fall back to the last configuration that worked.

Keep in mind that not all changes need to involve the router's configuration files or OS. For example, perhaps your company recently hired someone to straighten out that rat's nest of a wiring closet, and that person accidentally plugged the router into the wrong subnet when he or she put the closet back together. The wiring closet change should have been documented as a network change, and would tip you off that you need to check the router's interfaces to see what they are plugged into.

 There is no such thing as a minor change! Every single change to your network devices should go through your change management process. *No* change is too minor. We've all heard the story about the technician who blew dust out of a router's cooling fan. He blew hard enough to stop the fan (good lungs), causing the router to overheat and restart itself at seemingly random intervals. Had that simple maintenance action—cleaning out the router—been logged as a change, a senior administrator might have guessed that the problem was in the cooling fan, and checked that out first for a speedy resolution to the problem.

Of course, if you don't have a change management program in place or, at least, a backup of the router's configuration, you're out of easy options. You will need to start troubleshooting the problem the hard way, which might eventually involve completely reloading the router's factory configuration and rebuilding your configuration from scratch. Such drastic measures highlight the importance of both backups and a solid change management methodology.

Obviously, the easy way to always make sure you have a backup is to have a configuration management solution that does it for you. These solutions can detect—through technologies such as Syslog, Simple Network Management Protocol (SNMP), Remote Authentication Dial-In User Service (RADIUS), or Terminal Access Controller Access Control System (TACACS)—changes to your devices, and automatically download the latest configuration into a repository. You can analyze the differences between versions and roll back to any prior version any time you need to. In fact, these solutions often do a better job of answering the question “what has changed?” than a manual log would do, because they can tell you with a button click what has changed in a device's configuration. If the solution is enforcing a change management workflow for you, it can also alert you when out-of-workflow changes occur, letting you immediately focus on the potential problem.

Topic 4: Configuration Change Management Techniques

Q 4.1: Which new technologies can help ease network configuration management?

A: Until very recently, network configuration management has worked pretty much the same way it has for more than a decade: Administrators deal with devices on a case-by-case basis. To be sure, new tools have made it possible to use configuration templates, for example, to help ensure that all routers are configured consistently. However, by and large, network configuration management has always been a per-device activity. One problem with this reality is that it doesn't work well in environments that have different types of devices. For example, when a Cisco expert is looking at a Cisco device's configuration, the expert knows to look for certain considerations to make sure the device is properly configured. However, when looking at a Nortel device's configuration, the expert might easily overlook settings simply because he or she is unfamiliar with the different format. Because most organizations aren't homogenous—they use at least a few different manufacturers' devices—it can be difficult to manage devices consistently.

One way new technology can help is by abstracting devices' configurations into a vendor-neutral format. Rather than requiring administrators to work directly with a device's configuration, administrators can work—to a certain degree, at least—with an abstracted, vendor-neutral configuration. Although this approach doesn't work for *every* element of a device's configuration, it is especially helpful for consistency in security and other common areas of configuration. For example, Figure 4.1 illustrates how a solution might collect information on the SNMP community string information—a key security setting—from multiple devices, and represent that information in the same fashion. This format makes it easier for an administrator—who might not be experienced with every manufacturer's configuration format—to easily check for the correct, consistent settings.

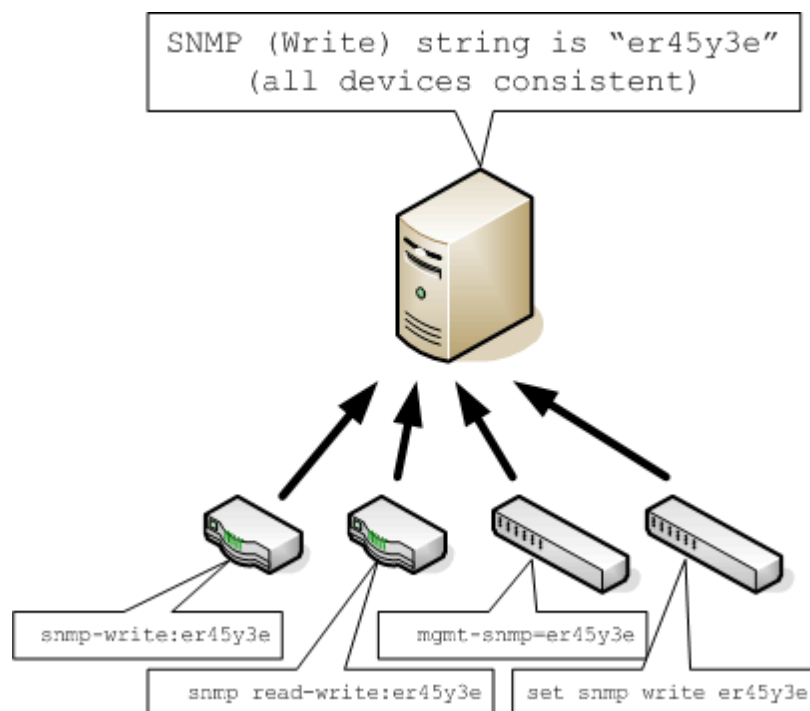


Figure 4.1: Displaying configuration information in a vendor-neutral format.

Many configuration management solutions can display details about changes made to a device; that capability is, in fact, a key part of most solutions. However, early solutions displayed the information simply as a difference between two configuration versions, as Figure 4.2 shows.


Original Configuration	New Configuration
<pre> aaa new-model TACACS -server host 192.168.12.42 aaa authentication login default tacacs+ aaa authentication ppp default tacacs+ aaa accounting exec start-stop tacacs+ aaa accounting network start-stop tacacs+ </pre>	<pre> aaa new-model TACACS -server host 192.168.12.43 aaa authentication login default tacacs+ aaa authentication ppp default tacacs+ aaa accounting exec start-stop tacacs+ aaa accounting network start-stop tacacs+ </pre>

Figure 4.2: Reviewing changes made to a device's configuration.

There is no intelligence in this report; it is simply an analysis of the differences between two versions of a text file, such as you might generate with a diff command-line tool. Such reports are extremely useful, but they again require someone who is familiar with the device configuration format to determine the actual business impact of the change.

A configuration management solution capable of abstracting this information into a vendor-neutral format can generate a shorter, more business-level report of the change, such as a simple statement: *The TACACS server address was changed*. This statement has immediate meaning to any technical professional familiar with network devices, regardless of whether the professional understands this particular device's configuration format. Native-format change reports will *always* be useful, especially for troubleshooting; abstracted change reports merely provide additional uses and make the configuration management solution somewhat more flexible. Newer configuration management solutions are beginning to offer configuration abstraction and are beginning to leverage that capability in change reports and in other areas of functionality.

One key area of functionality made possible by configuration abstraction is policy-based management. Current configuration management solutions can allow you to specify higher-level configuration policies in a *vendor-neutral format*. In other words, you're managing in a slightly more business-level fashion than a purely technical fashion because you can specify configurations in an abstract, vendor-neutral format. The solution then translates those policies into the appropriate per-device configurations, and implements the configurations on your devices in their native formats.

 This technique is discussed in more detail in tip 5.1.

New technologies are also helping network configuration management systems better integrate with leading enterprise management frameworks, such as IBM Tivoli and HP OpenView. By integrating tightly with these frameworks, the new technologies are enabling enterprise administrators and managers to work with a broader array of tools from within a single interface, streamlining network administration, improving consistency, and improving several operational metrics (including the all-important metric of network uptime).

Q 4.2: How can I back up all of my network devices?

A: Sadly, not many networks are built around one vendor's solution. You could simply implement each vendor's solution, and deal with the different techniques each uses to accomplish tasks such as device configuration backup. A better alternative, however, is to implement a solution that can simplify network configuration management by handling *all* your network devices, regardless of their manufacturer. One such solution is available from AlterPoint (<http://www.alterpoint.com>). Still another solution is ReadyRouter (<http://www.readyrouter.com>), a product designed to save device configurations automatically, restore them when necessary, and track changes made to them. A third is made by Voyence (<http://www.voyence.com>), which, like the other three, can detect and save changes automatically.

If you are fortunate enough that all your network devices came from the same manufacturer, the manufacturer probably provides some kind of software to help automate device backups, which is a key part of change management. Cisco Systems (<http://www.ciscosystems.com>), for example, offers a useful piece of software called the CiscoWorks Resource Manager Essentials (RME), which provides a Web-based interface for inventory management, change auditing, device configuration, and much more. RME works with most Cisco devices, from routers to switches. RME can inventory and monitor your Cisco devices, and report any changes that occur to their configuration, and much more.

If you don't want to invest in a commercial solution, you can probably cobble together something on your own. For example, most network devices support Trivial File Transfer Protocol (TFTP) for retrieving their configuration files; you can easily write a command-line script that queries each of your devices for their configuration files and saves them to a file server. You could even schedule the script (using cron on UNIX systems and Task Scheduler on Windows systems) to run on a regular basis, ensuring that you get a weekly or even nightly backup of your device configurations.

Unfortunately, many devices don't support TFTP. For those that don't, you will need to log on to the device and manually query its configuration, perhaps writing down the results of the query or saving them in a text file for future reference. A benefit of AlterPoint's product and similar solutions is that they can automatically perform the tedious task of collecting configuration data from devices that don't support TFTP or some other bulk-transfer method. In fact, one key shopping point for a commercial configuration management solution is vendor-neutrality, meaning the solution can work with many vendors' products, and relative technology-neutrality, meaning the solution supports several methods for retrieving configuration information from devices.

Topic 5: Selecting and Deploying a Network Configuration Management Solution

Q 5.1: How do network configuration management solutions support policy-based management?

A: Policy-based management is a new concept in information technology management that has been gaining traction in the area of operating systems (OS) management. It is relatively new in the realm of network device management, but can actually be more effective there because network devices typically have more accessible and less complicated configuration repositories than the average network OS.

Traditional management has typically involved the creation of policies governing how the network will be configured; technical professionals then translate those policies into specific configuration settings, and implement them on their devices. One significant problem with this approach is that it is difficult to quickly reconfigure the enterprise because devices must be individually reconfigured to meet changing needs. Configuration templates are often used to help mitigate the pain of individual device reconfiguration and to improve consistency; however, the fact remains that the devices need to be individually configured. Another problem is that per-device management doesn't accommodate *configuration drift*.

Configuration drift in network devices occurs primarily when changes are made outside of your normal configuration process. As Figure 5.1 shows, you start with a base configuration that meets your business policy requirements (including any compliance requirements). Out-of-process changes are made over time, leaving you *thinking* you're configured one way, but in reality, are configured differently.

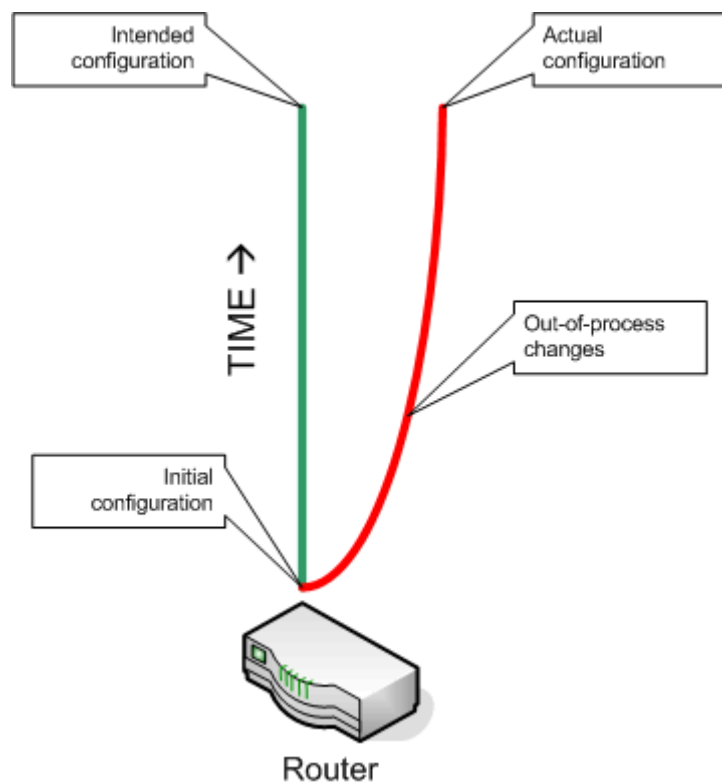


Figure 5.1: Configuration drift results from out-of-process changes.

The problem is simply that you're creating configurations to match policies, then trying to manually enforce the configurations. Policy-based management takes a somewhat different approach: You define technical-level policies that meet your business requirements, then a solution *enforces* those policies (or, at the very least, informs you when your devices aren't meeting your policies).

This difference in management style is subtle, but the ramifications are significant. For example, by establishing policies for what your device configurations should be like, you no longer have configuration drift. When configurations drift from the policy standard, you're notified immediately. In some instances, the configuration management solution might even be able to *remediate* the problem, reapplying your policy-compliant configuration in place of the non-compliant one.

Enabling an agile enterprise is also a key benefit of policy-based management. Want to change the Remote Authentication Dial-In User Service (RADIUS) server used by all your network devices? Simple: Change your policy. Your management solution will quickly determine that all of your devices are now non-compliant (with the new policy, that is), and can remediate them, reconfiguring them automatically to meet the policy. Your enterprise can thus be more adaptable to change, because you only need to redefine your policies. Figure 5.2 illustrates policy-based management.

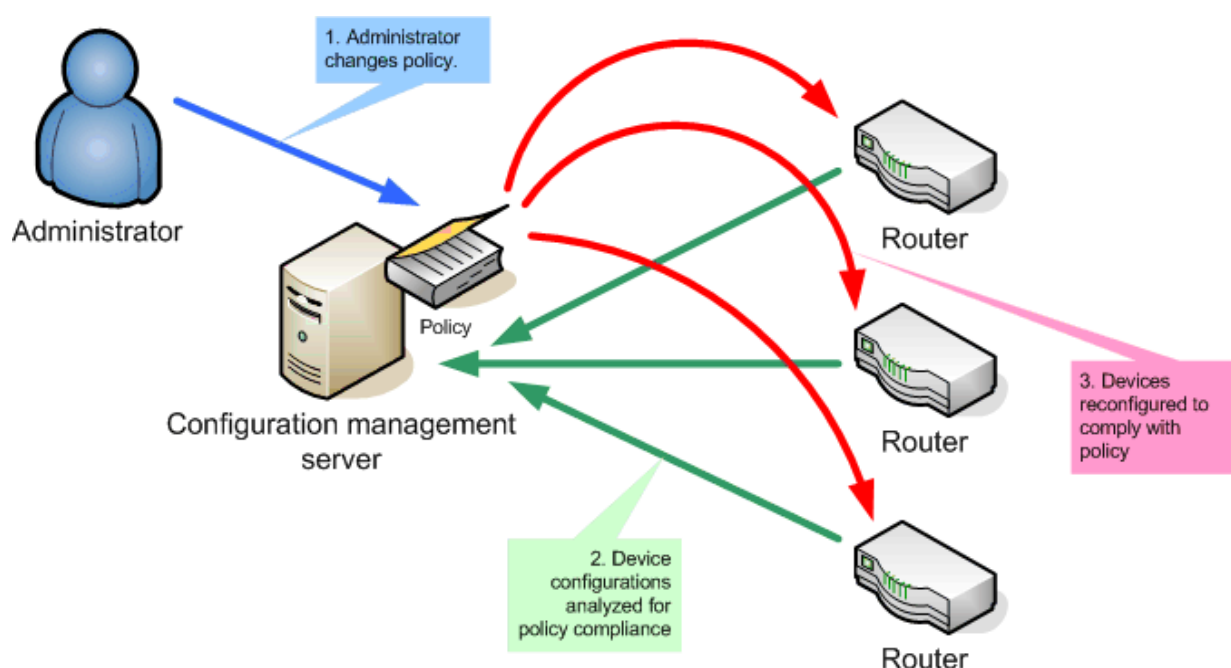


Figure 5.2: Managing devices through policies rather than direct configuration.

Policies are more complex and flexible than mere configuration templates. Generally, policy-based management combines with a layer of configuration abstraction, allowing policies themselves to be written in a vendor-neutral format; templates, in contrast, are typically vendor-specific.

In addition, multiple policies can be layered. For example, one policy might focus entirely on Simple Network Management Protocol (SNMP) community strings, while another might focus on RADIUS configuration. Policies can be applied to devices as-needed; routers might be subject to a policy regarding multicast boundaries, while switches might be subject to a different policy that deals with 802.1X configuration. Both might be subject to common policies such as SNMP configuration.



If you're familiar with how Microsoft Active Directory (AD) employs Group Policy to configure desktop computers, then you're familiar with policy-based management. An entire set of policies can be applied to groups of managed units (such as to desktop computers or, in the case of network management, to network devices); each policy states the desired configuration, then an enforcement mechanism ensures that the policy is met.

Today, most network administrators are a bit leery of letting an automated solution make automatic changes to their network devices. After all, the devices *are* the network; a misconfiguration can be costly. For now, allowing lower-risk policies to be automatically remediated is a good middle ground. For example, enforcing SNMP configurations won't break the network and can provide a significant security advantage. At the very least, however, policy-based management provides better alerts and notifications when policies *aren't* being met. Even if the management solution isn't automatically fixing things for you, it's at least letting you know—quickly—that something's wrong, allowing you to fix it yourself.

Topic 6: Enterprise Network Configuration Management

Q 6.1: How does policy-based management make it easier to manage a large numbers of devices?

A: One of the biggest network management challenges in an enterprise environment is maintaining consistency. With hundreds—or even thousands—of network devices to manage, ensuring that they remain consistently and correctly configured can be difficult, if not downright impossible. This challenge applies especially to service providers managing customer networks. With multiple networks to worry about—each having its own unique requirements and configuration standards—ensuring consistency can be a nightmare.

Configuration templates have long been used to help ensure consistency. Listing 6.1, for example, shows a portion of a secure Cisco IOS template written by Rob Thomas (you can find the complete template at <http://www.cymru.com/Documents/secure-ios-template.html>). As you can see, this template specifies several “best practice” configuration settings to create a more secure IOS within Cisco routers. The problem with a template is that it is only good for the initial configuration of a router. For example, this template configures the router to use Terminal Access Controller Access Control System (TACACS) for accounting and authentication; if your TACACS configuration changes, you can’t easily reuse this template to change only that one setting. Instead, you would need to change that one section of settings on each router.

```
! Secure router configuration template.
! Version 3.1
! @(#)Secure IOS template v3.1 17 NOV 2003 Rob Thomas robt@cymru.com
! @(#)http://www.cymru.com/Documents/secure-ios-template.html
!
! This configuration assumes the following topology:
!
! Upstream/Internet
! 5.5.5.1/24
!   |
! 5.5.5.254/24 (Ethernet 2/0)
! THIS ROUTER
! 6.6.6.254/24 (Ethernet 2/1)
!   |
! 6.6.6.1/24
! Firewall
! 7.7.7.1/24
!   |
! 7.7.7.0/24
! Intranet
!
! In this case, 7.7.7.5 is the loghost, FTP server, etc.
! for the router. It could also be the firewall if
! circumstances dictate.
!
service nagle
service tcp-keepalives-in
service tcp-keepalives-out
! Show copious timestamps in our logs
service timestamps debug datetime msec show-timezone localtime
service timestamps log datetime msec show-timezone localtime
```

```

service password-encryption
no service dhcp
!
hostname secure-router01
!
boot system flash slot0:rsp-pv-mz.121-5a.bin
logging buffered 16384 debugging
no logging console
enable secret <PASSWORD>
no enable password
!
! 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> password <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 6.1: A portion of a secure Cisco IOS template.

Network configuration management solutions can help deploy that change to hundreds of routers by allowing you to script the change—better solutions can even generate a script for you. But ease of deployment aside, you have now “violated” your original template, meaning you can no longer use it as a comparison point to determine whether your routers are properly configured. In short, templates are great for initial configurations, but they don’t help with the ongoing maintenance of the device.

Here is where policy-based management comes in. You might still use a template like the one that Listing 6.1 shows to help configure devices initially, but from there, a policy-based configuration management solution takes over. You define a set of *rules*, each of which relates to a single configuration setting. For example, you might create each of the following settings as a single rule:

- No service pad
- No IP source-route
- No IP finger
- No IP bootp server
- No IP domain-lookup

These rules are then combined into a *policy*, which in this example might be named “Disable unnecessary services.” The policy is then assigned, or applied, to one or more devices. Assigning the policy to a device causes the configuration management solution to alert you whenever that device falls out of compliance with the policy; some solutions might even provide for automated remediation, reconfiguring the device to meet the policy again without any intervention from you.

An effective network configuration management solution will allow policies to be assigned dynamically. In other words, policies would be assigned to all devices meeting certain criteria, such as a specific device OS (like Cisco IOS), a firmware version number, and so forth. The benefit of this dynamic assignment is that the policy can be made to apply to all devices that need it, without any intervention from you. If a new router is added to your network, the appropriate policies are *automatically* enforced, and you’re not required to manually apply them to the new device. Dynamic assignment therefore provides better consistency in your network’s configuration. By contrast, static assignment requires you to determine which devices require a certain policy and to constantly maintain your assignments as devices are added to and removed from the network.

Once in place, policies can provide a more effective means of managing large numbers of devices. For example, suppose you create a policy to enforce the correct TACACS configuration on Cisco devices. It might contain the same configuration settings as the template you use to initially configure devices:

```
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
```

If your TACACS server changes, you don't need to manually reconfigure each device. Instead, you simply change your policy:

```
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 7.7.7.10
tacacs-server key slurpee
```

All existing devices aren't configured this way, and therefore don't comply with the policy; the configuration management solution will detect this discrepancy and either alert you to non-compliant devices or, even better, remediate the devices' configurations and bring them into compliance—in other words, reconfigure them for you. Network configuration becomes a matter of simply maintaining your policies correctly, and allowing the policies to filter down to the devices in terms of the proper configuration.

Another major enterprise challenge is the array of devices found on the network, and the array of different manufacturers who provide those devices. Few networks are “all Cisco” or “all Nortel;” most use best-of-breed solutions and select routers, switches, firewalls, and other network infrastructure devices from a variety of manufacturers. This setup makes maintaining configuration policies more challenging because you might need to maintain multiple versions of each policy to represent each different device vendor. Network configuration management solutions can help by providing configuration *abstraction*, a process whereby vendor-specific configuration settings are displayed to you (in a “policy builder” of some kind) as vendor-neutral information. The solution then translates those policies upon application, as Figure 6.1 shows, into the vendor-specific configurations. Because the solution understands the different configuration settings, you don't need to; you can maintain a single set of abstract policies and let the solution worry about how to physically implement them.

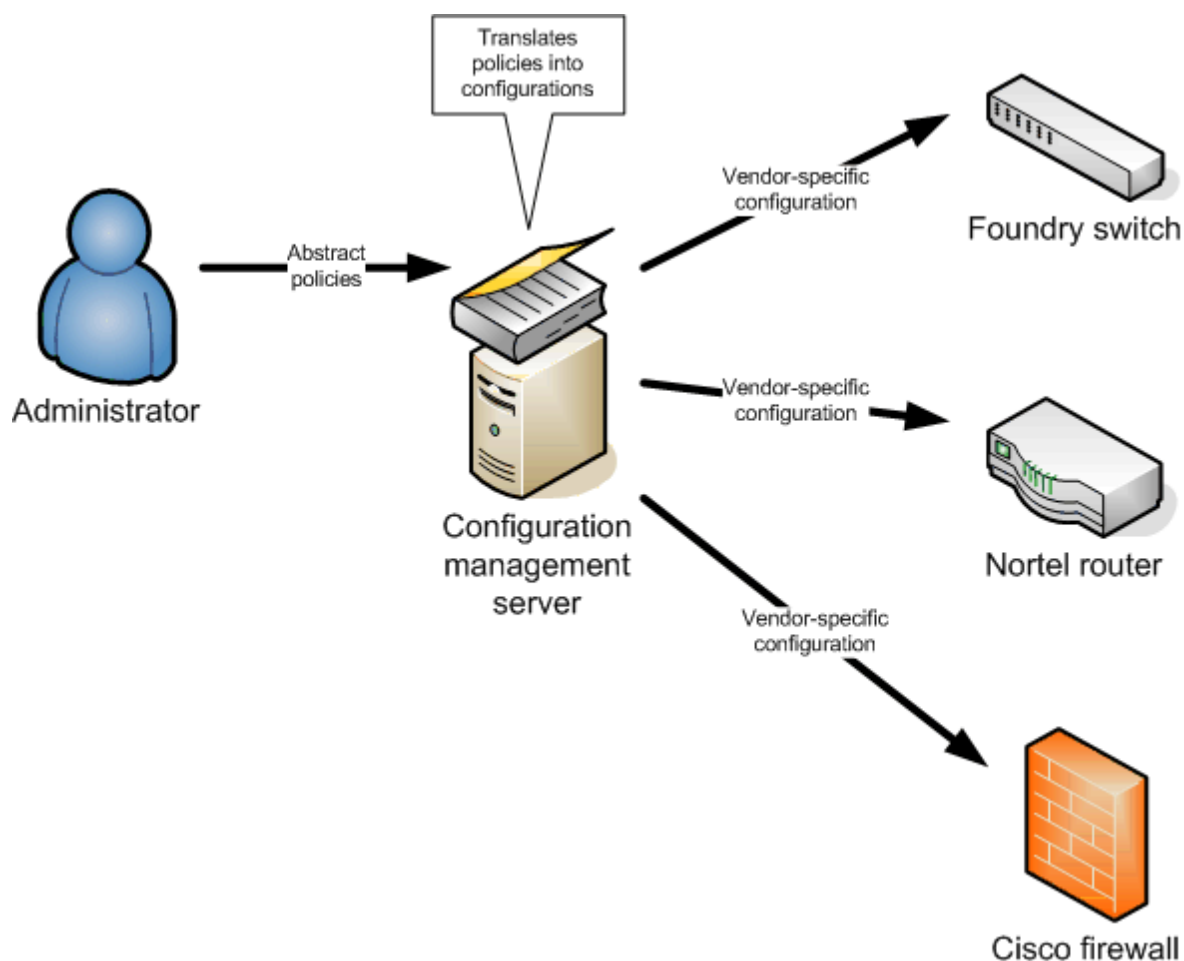


Figure 6.1: Translating abstract policies into configuration settings.

The ideal network configuration management solution will combine abstraction with policy-based management to provide easier, more consistent, single-seat administration for any number of devices. It may even be able to discover additional devices as they are added to the network (device discovery is a common feature) and apply the necessary policies, ensuring that your network always remains configured the way you want it to be.

Topic 7: Compliance Management for the Network

Q 7.1: How can policies help us better manage regulatory compliance for our network?

A: Most regulatory compliance requirements—such as those of the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act, 21 Code of Federal Regulations (CFR), various European Commission rulings, and so forth—revolve around two central themes: security (often referred to as privacy) and accountability. The driving philosophy behind these regulations is to provide protection for sensitive data (such as healthcare or financial information) and to provide a layer of accountability so that all access to this sensitive data is recorded and can be tracked.

Network infrastructure devices don't usually need to worry about direct data access or accountability; however, because the network transmits all of that data, the network obviously plays a role in protecting the data's confidentiality. Thus, network devices need to be configured to provide the necessary privacy. They also need to be configured to provide the necessary auditing so that any changes to the devices' configurations that might compromise privacy can be tracked.

As I've discussed in other tips, most network devices have fairly primitive internal capabilities when it comes to logging device access; instead of building logging databases into devices, the industry has evolved around external technologies such as Terminal Access Controller Access Control System (TACACS) and Remote Authentication Dial-In User Service (RADIUS), which receive *accounting*, or logging, messages from devices and store them in server-based databases. None of these logging technologies typically provide a sufficient level of detail with regard to which changes are made in a device—they tend to focus primarily on administrative access to the device, not what the administrator does once he or she is in. Network configuration management solutions can use the logging messages as a sort of trigger. The messages inform the solution that an administrator has accessed the device (and might therefore have made changes), so the solution can pull the device's configuration and look for changes.

All of this activity, however, depends entirely on the device being configured to send those logging messages. A Cisco router can be configured to use TACACS, a popular logging technology, with a configuration similar to the following:

```
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
```

The same router could be configured to use syslog with the following configuration:

```
service timestamps log datetime localtime
no logging console
no logging monitor
logging 192.168.1.100
```

Cisco Catalyst switches would use a slightly different configuration for syslog:

```
set logging server enable
set logging server 192.168.1.100
set logging level all 5
set logging server severity 6
```

Cisco PIX firewalls have an even different syslog configuration:

```
logging on
logging standby
logging timestamp
logging trap notifications
logging facility 19
logging host inside 192.168.1.100
```

The point in listing three syslog configurations for devices from a single manufacturer is to highlight that all the configurations are different and that maintaining those configurations on a network with multiple *vendors* can be difficult to say the least. This arena is where policy-based management applies.

The bottom line is that it is critical that certain device configuration settings remain in place in order for your network to remain compliant. Ensuring that configurations remain in place can be a daunting manual task. You must become familiar with a *lot* of different configuration files and you need to look at them *constantly*; being out of compliance for even a single moment means that someone could reconfigure a router and lower its security without being noticed.

Policy-based management can automatically alert you to devices that aren't compliant, and can even automatically reconfigure those devices to be compliant again, removing the possibility for auditing to be turned off without someone at least being notified of the problem. If your network configuration management solution also supports configuration abstraction, you'll only need to configure the policy *once*, using a vendor- and device-neutral syntax; the configuration solution will translate that into device-specific configuration settings as necessary and implement the policies for you. In short, policy-based management is the single most effective tool you can have to ensure your network remains compliant.

Q 7.2: What does my network configuration have to do with compliance?

A: These days, the word *compliance* is used as a shortcut for *compliance with legal requirements*, and typically refers to some industry-specific regulations or legislation dealing with information management; examples in the United States include the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act, 21 Consolidated Federal Rules (21 CFR), the Graham-Leach-Bliley Act, and so forth.

The connection between these rules and your network configuration can be subtle. Generally speaking, these laws concern themselves with the security, privacy, and accountability of specific types of information. HIPAA, for example, is all about patient information in the health care industry; Sarbanes-Oxley deals primarily with financial information and practices for auditors. Their broad goal is to ensure that all data is maintained as confidential, access to data is controlled and monitored, and access to data is *accountable*, meaning you can always look back and see who accessed what and what changes they made, if any, to data covered by the rules.

It's easy to see how network file servers become involved, because they store a lot of the data these laws are concerned with. But how does data go to and from file servers? The network. Thus, if someone could compromise your routers, that person could in theory gain access to every byte of data that passes through those routers. Hence, your routers need to be secured. In order to maintain that security, every change to a router's configuration needs to be examined to make sure it doesn't compromise the router's security. Every change needs to be *accountable* so that any changes that *do* compromise security can be traced to the guilty party. A Sarbanes-Oxley Report, for example, might detail every change made to every network device in your environment, along with information about when the change was made, who made it, and the details of the change. Such a report would help an auditor examining your Sarbanes-Oxley compliance to review changes and ensure that they were all made within the scope of a configuration management process—that is, changes were reviewed for their security implications, approved by management, and deployed as planned.

HIPAA carries roughly similar requirements, including the requirement that anyone in possession of health care records provide a report of all disclosures of those records. As it would be nearly impossible to record disclosures made accidentally over the network—such as through a network device such as a switch or router—you have to make sure such disclosure can't occur. Again, this means a secure configuration and complete accountability for all changes made to the configuration.

These are all difficult tasks without the help of a decent configuration management solution, such as those offered by companies such as AlterPoint (<http://www.alterpoint.com>) and Voyence (<http://www.voyence.com>). High-end configuration management solutions are designed to detect changes to device configurations, report on those changes, and even undo unauthorized or improper changes. They can also help enforce a configuration management workflow process, which ensures that changes are properly reviewed, approved, scheduled, deployed, and logged for auditing purposes.