[**Editor's Note:** The following excerpt is from Volume 2 of the free eBook *The Tips and Tricks Guide to Network Configuration Management* (Realtimepublishers.com) written by Don Jones and available at http://www.alterpoint.com/ebook/.]

Q: How can change management improve network security?

A: "Hey, we just need these holes opened in the firewall as a test, then you can close them again." How often have you had a similar request? So-called "temporary" changes are a common occurrence in most networks, even if they're only made to troubleshoot other problems. Unfortunately, these temporary changes often have a way of becoming permanent through neglect. Perhaps the administrator who made the change did so on Friday afternoon and forgot to undo the change the following Monday. Or maybe the change needed to be in place for a week, and everyone simply forgot to undo it. In some cases, those changes might not seem important, but they can add up: Administrator Joe makes one minor change, and Administrator Sally makes another; separately, neither change is a problem, but together they allow the world to access the company's private network.

Change management can help. First, a good change-management process ensures that all changes are reviewed by some central party so that dangerous change interactions can be detected before they're made. By documenting changes, a good change-management process can ensure that temporary changes are removed at the earliest opportunity. To provide these extra security precautions, your change-management process must consider the following factors for *each proposed change* to a network device:

- What other pending or temporary changes might interact with the proposed change to create an insecure situation?
- When will the change be undone, if ever? Who will be responsible for undoing the change? Both the responsible party and another administrator should set reminders to both undo the change and review the affected devices' configuration files to verify the removal.
- Some changes, especially those made for testing purposes, might be very short-lived. In those cases, you might be able to use a configuration tool (either provided by your device manufacturer or a third party) to automatically restore devices' original configuration after the change is no longer needed, ensuring that an administrator doesn't forget to make the change.

A change-management process should also include periodic device configuration audits. These audits can help spot potentially insecure configurations that weren't caught by the up-front change-management process. With experience, you'll build a checklist of concerns that you can use during a configuration audit, such as commonly opened ports, router-configuration mistakes, and so forth. Bulletins from device vendors might call attention to potential security and configuration problems, and those bulletins can be incorporated into your device configuration audits to improve the overall security of your network.

Q: How will wireless devices change the way I secure network devices?

A: With the widespread adoption of wireless networking by many businesses, network security is more of a concern than ever. Of course, wireless networking (particularly the prevalent 802.11x standards in use by most companies) offers security features. The Wireless Encryption Protocol (WEP), for example, helps ensure that only authorized users attach to a network to begin with, regardless of their ability to authenticate to network devices. WEP is a *must* if you manage your network devices over a network accessible to wireless users. Why? Without WEP, anyone can see the packets sent across a wireless network, and those packets might include the configuration passwords of your network devices—passwords that are often sent in clear text when you Telnet in to make configuration changes. WEP protects the network by allowing only authorized users to attach.

However, the very idea that passwords might be transmitted in the open gives me the willies and is all the more reason to establish a dedicated, *wired* network for network device management. This dedicated network can be configured with its own firewalls so that only authorized administrators can even access the network, and a hardwired network eliminates any potential for passwords being intercepted by wireless eavesdroppers. Even wireless devices, such as wireless access points (WAP), should be managed via a wired network whenever possible. Figure 2.1 shows a model network configuration with network devices connected to a separated, dedicated, wired network designed for network management.

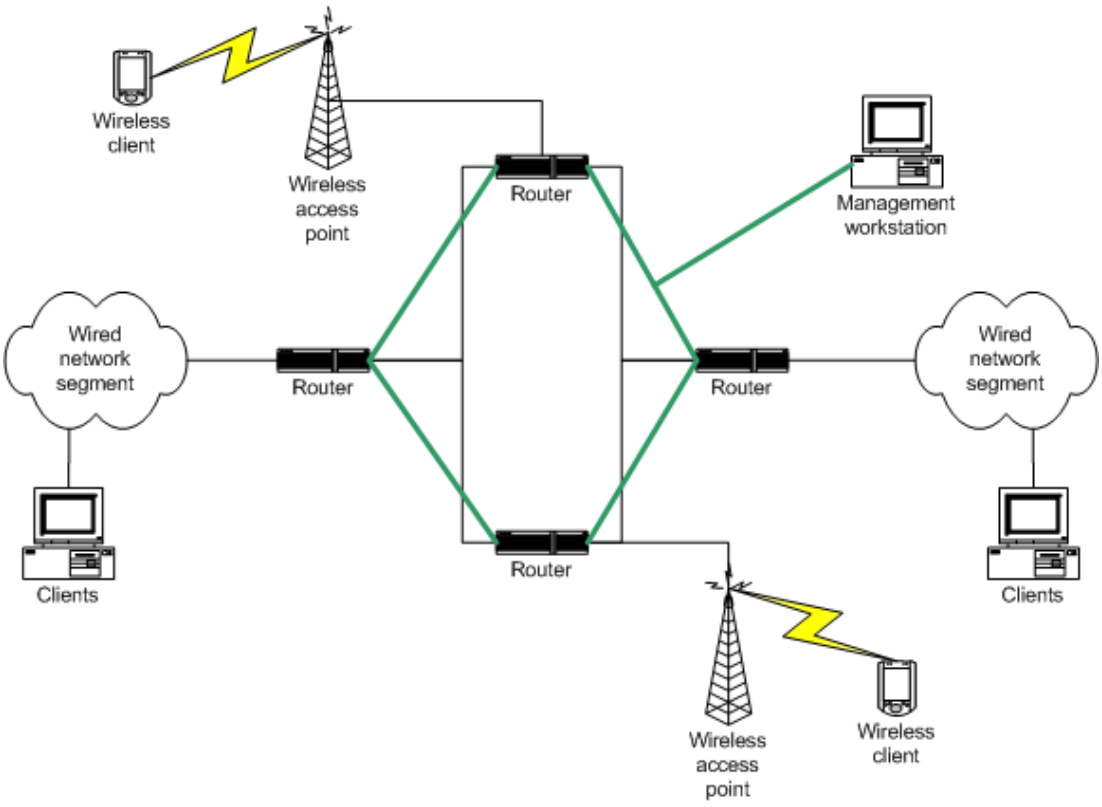

Figure 2.1: Dedicating a network to network device management.

The potential ability for someone physically outside of your company's buildings to access your network devices and make configuration changes is yet another argument for having a comprehensive, software-supported change-management process in place. Change-management software that can automatically archive device configuration backups will let you recover more quickly in the event that your wireless network is hacked and used to upload inaccurate configuration information to a network device.

Sure, with 128-bit (and now, 256-bit) WEP encryption and other wireless security protocols including 802.1x, well-chosen device configuration passwords, and other security measures, the odds of a wireless hacker ruining your routers is slim. But the most secure networks are run by rampant paranoid administrators who take every possible precaution; we'd all do well to learn from their example and take no chances.

[**Editor's Note:** This content was excerpted from the free eBook *The Tips and Tricks Guide to Network Configuration Management* (Realtimepublishers.com) written by Don Jones and available at http://www.alterpoint.com/ebook/.]