Realtime
publishers

The Shortcut Guide™ To

Smart Network Management for the SMB

sponsored by

Chris Hampton

Copyright Statement

Chapter 3: The Key to Smart Configuration and Change Management

An increase in the use of diverse network technologies, plus the introduction of virtualization throughout the network architecture, multiplied by the number of users demanding flexible access to the network equals what? The answer is *complexity*. No, this is not a child's homework problems—this is reality for many SMBs. If you have not felt the pain of this scenario within your SMB, it may just be around the corner.

Today's network environments are becoming more complex. SMBs are seeing the introduction of additional types of network devices that were typically relegated to the larger corporations. More applications are moving to tiered architectures with multiple load-balanced systems. SSL/VPN solutions are becoming more critical to production as more of the workforce goes mobile. The use of layer 3 core switches with added routing functionality and the wide use of VLANs present additional complexity into the network.

For years, SMBs have manually managed the devices across the network, including firmware upgrades, patches, VLAN provisioning, ACL updates, and configuration updates and changes. This method worked fine when the number and type of devices stayed small, but such is not the case today. The process of manual configuration and tracking all network devices adds an unnecessary burden, wastes time, and introduces risk with common errors such as typographical mistakes or incorrect cut and paste tasks.

Virtualization is becoming the hottest trend in the IT industry and many SMBs are seeing the business value in moving to a virtual server infrastructure. From the network management perspective, virtualization brings a new layer of complexity with the blending of physical and virtual networks. Also, the use of virtual network appliances is growing and adding to the list of devices that require configuration and management.

Users are also changing the way they interact with the network; the days of rows of cubicles populated by employees working an 8-hour shift safely behind the corporate firewall are gone. Today, businesses are adjusting to end users that are demanding anytime, anywhere access to the network. The network architecture that supports this business model is more complex. Stable access and high performance of the network becomes more critical to the business as more users move to a flexible access model.

As the types of network technologies increase and reliance on the network becomes more critical to the business, you need a solution that will ease the administration of the network while providing a higher level of consistency. When evaluating a network management system, the benefit of a smart configuration and change management option cannot be overlooked.

Simplify Your SMB's Network Configuration Management

It's late Friday afternoon and IT just found out that the Western regional network administrator has left the company and they must change passwords on all routers and network switches across the company's 20 branch locations before they can leave for the weekend. This task may not sound too cumbersome initially, but as you begin to understand how most small businesses currently manage their network devices, it will become clear that the task is a very difficult process.

Such an SMB with 20 branch locations might have a firewall device, a WAN router, and a pair of network switches per location. Most of the time, these devices are obtained from different vendors (3Com, Cisco, HP, Fortinet, and so on)—different vendors often means different configuration environments. The process of changing the password on each type of device requires differently structured command syntax. Now multiply those four devices in each branch location by 20 branches, and there are at least 80 devices to log into, determine the correct syntax to change the password, and save the configuration.

That is, if IT even has record of the current passwords on each device in the network. Without a consistent way to track passwords across devices, many businesses face the ugly proposition of recovering lost passwords before even beginning this process, especially when key IT employees leave and important passwords were never documented. The simple task of changing the password on each device across branch locations just got a whole lot more difficult.

A smart network management system can dramatically change the way an SMB approaches configuration and change management. In this chapter, the following key features and benefits of a smart network management system with regard to configuration and change management are presented:

- *Centralized configuration management*—By centralizing all device configurations, management of the network becomes much easier. More importantly, by centralizing device configurations, standardization and adherence to compliance standards become possible.
- *Secure configuration and change management*—With a diverse infrastructure including different types of network devices and multiple vendors, the process of providing secure configuration updates is difficult. Broad support for multiple secure protocols and centralized mapping of device security information eases this process.

- *Power of integrated alerting and reporting*—Through integration with the alerting and monitoring technologies within the smart network management system, configuration management changes can be tracked. This feature will help to minimize unplanned changes and detect unauthorized access to network devices.
- *Automated configuration task and monitoring*—The automation of repetitive configuration tasks across multiple devices makes possible significant reduction in configuration errors. Standardization of device configurations can also be achieved. Integrated monitoring of configuration task executions will simplify tracking of changes and troubleshooting.

Configuration Management

The scenario outlined earlier occurs across many SMBs every day. The core problem lies in the decentralized configuration management of the network. Networks within most SMBs have grown over time. Initially, the SMB had a single location with a router, a couple of switches, and a few workstations. In the beginning, managing these few devices manually made sense. As the network grows and additional locations come online, the practice of using a decentralized manual approach to device management falls short.

As Figure 3.1 shows, manual configuration and change management requires the painstaking task of touching each device to update the configuration file and then moving on to the next device. Often the devices have different login credentials, each requiring additional manual tracking. In a decentralized configuration management environment, network administrators have to refer to saved spreadsheets for credentials, manually login into each device, copy configuration files back and forth between text files, make manual changes, and finally upload the text files to the device to submit the changes. This process is timely and prone to errors.

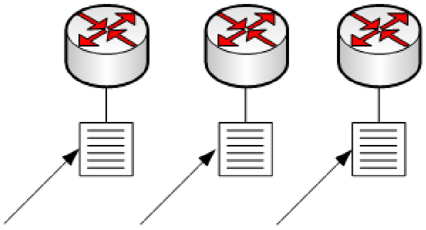


Figure 3.1: Decentralized configuration management.

In contrast, a centralized configuration management environment (see Figure 3.2) entails copying the individual device passwords and configurations to a central database within the network management system. A centralized configuration management environment greatly reduces the time involved in saving and changing network configurations. Accuracy of the configuration changes is also increased, and a higher level of consistency can be achieved.

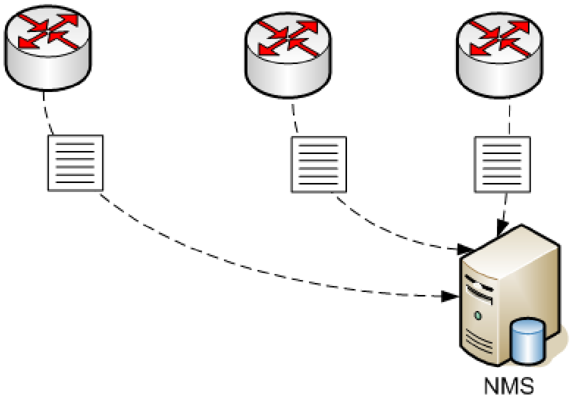


Figure 3.2: Centralized configuration management.

A major advantage in a centralized configuration management environment is the ease at which large-scale device updates can be completed. Looking at the earlier example, Figure 3.3 depicts a decentralized configuration management environment. The network administrator has to access each router login (device 1), change the password, save the configuration, and log out of the device, and then complete the same set of steps for each switch (device 2) and each firewall (device 3). This process is then repeated across every device at each location for a total of 80 devices. Even in a case where the network devices are from the same vendor and same model, the need to manually access each device and execute the four simple commands still requires significant effort and time to complete.

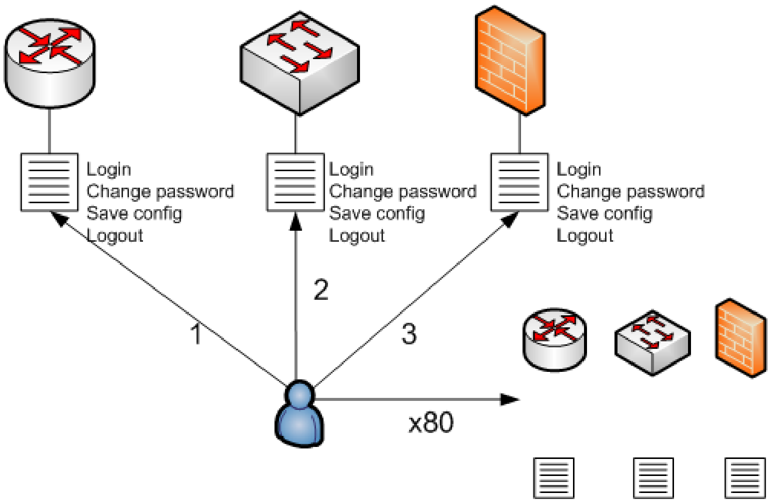


Figure 3.3: Decentralized configuration changes.

Smart network management systems incorporate centralized configuration management. Instead of manually copying device configurations into text files and tracking device passwords in multiple spreadsheets; a central database is used to store the configurations, passwords, and device information. With the centralization of configuration data and passwords, the process of updating multiple devices becomes a much easier task. As Figure 3.4 shows, centralized configuration management reduces the time and effort by leveraging the central database and using scripted or schedule updates. In this example, the network administrator completes a configuration update across multiple devices in a single step, reducing the effort needed to touch 80 devices. With configuration data and passwords stored centrally, synchronization of like device types and models can be used to speed configuration changes.

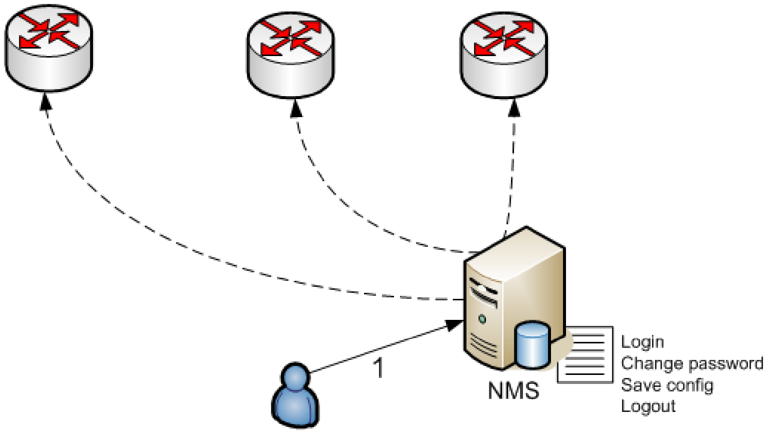


Figure 3.4: Centralized configuration changes.

Centralization of Passwords and Authentication

In many SMBs, as the number of devices continues to increase, the overwhelming task of tracking passwords and secondary authentication credentials can be daunting. Utilizing a smart network management system, IT can configure a centralized library of device credentials and passwords that are stored in a secure central database. The database can then be referenced when access to the device is required. Automation scripts and scheduled tasks can also reference the saved authentication credentials to speed the configuration update process.

By centralizing device authentication credentials for every device, an SMB can rest assured knowing that unexpected turnover or absence of a key employee will not cause a major interruption of network configuration management. Additionally, by storing authentication credentials in a secure database, alignment with industry compliance standards can be maintained.

Centralization of Device Configuration Backups

Network device configurations can be complex, involving hundreds of lines of text. If a device experiences a hardware failure, or if by human error a configuration becomes corrupt, having a recent and known good backup is critical. Many devices also maintain a running and saved configuration; these may be different depending on the status of the device changes applied.

An additional benefit of centralization within the network management system is central configuration backup. The scheduling and collection of each device configuration and storage in a central database increases the overall network availability. Prior to implementing a smart network management system, if a device failure or configuration corruption were to occur, the SMB would have to manually reenter the configuration by relying on saved text files and installation notes.

This process is slow and fraught with possible errors. With the use of centralized configuration backup, if a device failure occurs, the process of retrieving a known-good configuration from the central database and applying the saved configuration to the device reduces the amount of time the device is down and ensures accuracy in the re-configuration.

Scheduled Backups

Network device configurations can be negatively affected by any type of change. Add-hoc configuration changes, vendor firmware updates, or unplanned power outages—each of these scenarios can cause a device outage. To offset the effect of these types of outages, regular scheduled configuration backups should be completed on every device. Performing configuration backups at scheduled intervals such as weekly or monthly will ensure a recent backup is available for recovery if needed.

When evaluating a network management system, ensure the device configuration backup feature allows for scheduled backups on a daily, weekly, and monthly basis.

Secure Configuration and Change Management

Making the tasks of configuration and change management easier by saving and tracking device configurations centrally is only half the picture. Security of device access and configuration changes is very important. Think of a network environment where configuration and change management is approached in an ad-hoc manner. In such an environment, device logins and passwords may be stored in text documents or spreadsheets on a network share, no access control is in place to manage who has rights to change configurations, no support for secure network access to devices for updates is provided, and configuration changes are made in clear text across unsecure Internet connections.

The security risks introduced as part of an ad-hoc configuration management environment are many. As previously mentioned, the use of text documents and spreadsheets to store and track device credentials is one of the primary concerns. Although this solution seems to work fine for the first few devices, as the network grows, this manual process of securing logins, passwords, and configuration data becomes unwieldy. The centralization of passwords in a secure database provides the scalability and security required for network device password management. In like fashion, the centralization of device configuration data provides a secure and retrievable location for important configurations. With no support for secure protocol access to network devices, the SMB risks compromising device logins and passwords.

A smart network management system should include security features that address these areas of concern. Among the features to look for:

- *Secure protocol support*—By incorporating protocol access via SNMP v2, v3, SSH2, and TFTP, SMBs can maintain secure access to network devices, reducing the exposure of sensitive login and password information.
- *Centralized authentication management*—Centralization of critical device login and password information in a secure database is a very important security feature.
- *Centralized device configuration management*—Automated or scheduled backup of device configurations within a secure centralized database will help speed recovery during device failure and assist with standardization of configurations.

Is a Centralized Database More or Less Secure?

You may be asking yourself, "If all the network device authentication credentials and passwords are stored in one location, isn't the network even more vulnerable to attack? A would-be attacker would simply need to access the central database to gain access to every device on the network, right?"

With today's relational database software, the ability to access the central database is not as easy as it seems. With fully-integrated Active Directory (AD) authentication, strong password policy enforcement, password expiration enforcement, and SSL-secured network connections during authentication, it is not an easy task to gain access to the database credentials.

After authentication comes authorization. Relational database software uses a granular permissions model. Login accounts are only granted specific rights to the databases required.

The final layer of defense in a secure relational database is encryption of the data itself. Utilizing encryption technologies such as Transparent Data Encryption, critical data can be encrypted as it is written to the database and unencrypted when read from the database. These technologies utilize a secure system of encryption keys generated and managed at multiple levels within the relational database software.

Together, these three layers of defense authentication, authorization, and encryption provide a highly secure environment for the centralized storage of network device credentials and passwords.

Device Management

To this point in the chapter, the discussion has focused on high-level features a network management system should include with regard to configuration and change management. Where the "rubber meets the road" during day-to-day operations of the network, success is measured at the individual device level. When it comes to device configuration management, there are four key areas of focus:

- *Compare and contrast device configurations*—Provide quick and accurate troubleshooting of configuration data
- *Rapid recovery of device configurations*—Apply or repair device configuration files from central backups
- *Logging of device configuration changes*—Provide centralized logging of changes for audit and control
- *Notification of device configuration changes*—Enable proactive alerting of device configuration changes

Compare and Contrast Device Configurations

As mentioned earlier in this chapter, the backup of device configurations in a central database is critical to daily device operations. By utilizing the saved configurations, an administrator can conduct a *compare and contrast* between the saved configuration and the current running configuration to assist with diagnosing a device failure or related network failure.

To highlight this feature, consider the following example in which a network edge router was recently edited and configuration changes were implemented. After the configuration changes were made, connectivity to the Branch2 office was down. By using the compare and contrast functionality of the network management system, the administrator can quickly see where the configuration has been altered (see Figure 3.5).

Saved Configuration:	Running Configuration:
Current configuration:	Current configuration:
!	!
version 12.1	version 12.1
!	!
hostname HQEdge	hostname HQEdge
!	!
interface Serial0/1.1 point-to-point	interface Serial0/1.1 point-to-point
description link to Branch1	description link to Branch1
ip address 10.1.1.2 255.255.255.252	ip address 10.1.1.2 255.255.255.252
ip router isis	ip router isis
tag-switching ip	tag-switching ip
frame-relay interface-dlci 201	frame-relay interface-dlci 201
!	!
interface Serial0/1.2 point-to-point	interface Serial0/1.2 point-to-point
description link to Branch2	description link to Branch2
ip address 10.1.1.10 255.255.255.252	ip address 10.1.1.10 255.255.252.252
ip router isis	ip router isis
tag-switching ip	no tag-switching ip
frame-relay interface-dlci 203	frame-relay interface-dlci 203
!	!
end	end

Figure 3.5: Example of compare and contrast device configuration.

After reviewing the saved and currently running configurations, the administrator can quickly see that the IP address subnet masking was set incorrectly and the tag switching for forwarding of IP packet data has been disabled. The administrator can take immediate action to correct the running configuration and reestablish connectivity to the Branch 2 office.

Without this type of configuration tracking and visibility, troubleshooting an issue like this would take significantly longer. The administrator would have to hope that documentation of the frame relay network is up to date, then spend time going through the router configuration file line by line evaluating every setting. For many devices, this could mean hundreds if not thousands of lines of configurations.

Additional Benefit of Compare and Contrast

A secondary benefit of the compare and contrast feature is the ability to review the configuration files from two devices. For example, if your SMB is in the process of implementing a Voice over IP (VoIP) phone system, each branch location will require a separate network switch for the VoIP phones. The switch configurations will be very similar, and the switch hardware utilized is often from the same vendor and model. Once the switches are deployed and the VoIP system is up and running, incorrect configuration changes can cause the loss of communication across the entire organization.

The compare and contrast feature is beneficial in environments that utilize the same hardware type or model across many locations. By reviewing device configurations side by side, a quick determination can be made into which devices may have been misconfigured.

Rapid Recovery of Device Configurations

If a device failure occurs due to configuration corruption or unplanned configuration changes like the earlier example, the administrator needs a way to recover the device quickly. Traditionally, the process of recovery is more of a manual task; if the administrator was cautious, she may have taken the time to copy the configuration of the device to a text file before making changes. Many times, the administrator will sidetrack this step and make the configuration changes in the running configuration, test the changes, then commit the running configuration to the device's non-volatile memory (NVRAM).

What Is the Running Configuration?

On network devices, such as a router or switch, there are two areas of memory where configuration data can reside. The first area is the volatile memory; the running configuration is loaded in this memory area and any changes made at this level are lost if the device is powered down. The second area is the NVRAM, the saved or startup configuration data is loaded in this memory area. Once the configuration data is saved in NVRAM, the device can be powered down and restarted and the saved configuration will load back into volatile memory.

The problem with this approach is that some configuration changes cannot be fully tested in the running configuration and issues will only come to light during a device restart. At this point, the administrator can fall back to the text document with the copied configuration data for recovery. That is, if he took the time to create the text document before making any changes to the device.

By utilizing a scheduled backup of device configuration data to a central database, the administrator can easily select a known-good version of the device configuration and apply the saved configuration to the device, allowing for rapid recovery. This capability dramatically lowers the risk to the business for unplanned downtime and reduces the effects of human error.

Logging of Device Configuration Changes

Increasingly important to SMBs in a competitive market is the ability to ensure accountability and compliance with industry standards. A number of industry compliance standards such ISO27K's Information Security Management System and the Sarbanes-Oxley (SOX) Act call for a proven system of change auditing across each network device.

By leveraging a smart network management system that monitors each device, a detailed audit trail of configuration change data is logged to a central database. The log data includes such details as the exact configuration file that was changed, the date and time of the change, and what user account made the change. This data also helps to ensure that only authorized personnel are making changes to the network devices. Unauthorized configuration changes can be detected through this process by working in conjunction with alerting and notification, and can then be rolled back to maintain compliance.

Notification of Device Configuration Changes

Unauthorized configuration changes can cause major outages across the network and negatively affect business continuity. With that said, it is critical to proactively detect unauthorized changes before they become a major issue.

Many network devices generate syslog messages whenever their configuration undergoes a change. By listening to these messages, administrators can detect any configuration change in the device. A good example of the power of this feature is the management of edge devices such as Internet-facing routers. These devices are critical to the connectivity of the business network to the Internet, and any unplanned outages of these devices can be very disruptive to the business, affecting employees and customers.

Through the implementation of a device configuration change monitor that uses syslog alerts, a device change event can be flagged and alerted. IT personnel can then take action by initiating a device configuration comparison of the saved device configuration within the system management database and the device's running configuration. IT personnel can then roll back the unauthorized change. This process is depicted in Figure 3.6:

- Step 1—An unauthorized change is made.
- Step 2—A syslog alert is captured and sent to the network management console.
- Step 3—IT staff complete a device configuration comparison and initiate a configuration roll back by applying the saved configuration from the network management database.

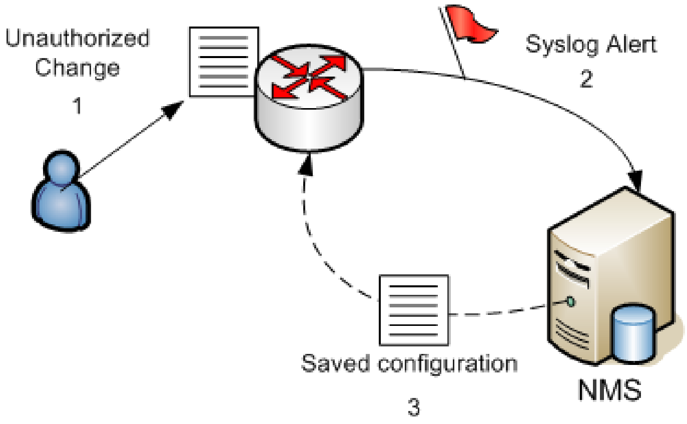


Figure 3.6: Device configuration monitoring.

The network management system should provide monitoring and alerting of key configuration change logging. In addition, intelligent notification should be available to allow for escalation of alerts to key personnel.

Scheduled Tasks and Script Execution

For an SMB, the responsibility of managing the configuration changes across an increasing variety of network devices can be a challenge. Often, with multiple vendor devices, the configuration file format, command syntax, and access credentials vary. With the importance of standardization and industry compliance—consistent and validated configuration changes must be maintained.

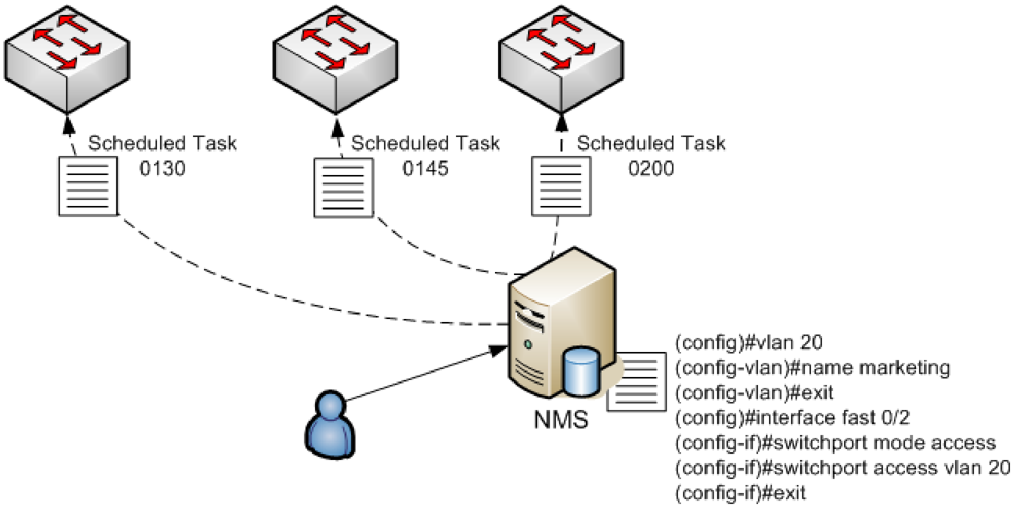
As the network grows in complexity and the number of devices increases, the use of simple manual configuration changes becomes too difficult and time consuming. What is required is a network management system that offers advanced features in the areas of scheduled tasks, automated configuration, and scripted execution. These features allow the administrator to focus on network optimization, trending, and growth planning instead of wasting time on repetitive configuration tasks across multiple devices.

Automating the Management of Device Configurations

Making a configuration error is easy when managing multiple devices through a manual process. Most configuration changes must be coordinated across multiple devices. For example, when a new VLAN is implemented within the network, each related network switch configuration must be updated with the correct VLAN ID, port number assignments, and required VLAN trunking. An error on a single switch configuration can affect the entire network.

Connectivity errors are obvious, but other configuration mistakes can introduce more subtle errors, such as reduced performance or a security vulnerability, which may persist for weeks or months until discovered. The use of automated configuration management can substantially reduce the percentage of outages caused by configuration errors. Through the use of automation, manual and repetitive tasks are eliminated, greatly reducing the time and man-hour cost of configuration management. Network administrators and managers can set up scheduled tasks to roll out configuration or password changes to existing devices; provision a new device with a standardized configuration; or restore baseline configurations to one or more devices if changes need to be rolled back.

When automated configuration management is used to complete the VLAN addition in the previous example, the opportunity for errors is reduced and standardization of configurations is guaranteed. As Figure 3.7 shows, a single configuration update is made by the administrator within the central network management system, then a scheduled task is assigned to each switch to complete the update.



```
(config)#vlan 20
(config-vlan)#name marketing
(config-vlan)#exit
(config)#interface fast 0/2
(config-if)#switchport mode access
(config-if)#switchport access vlan 20
(config-if)#exit
```

Figure 3.7: Automated configuration management.

The Power of Script Execution

When attempting to implement an automated configuration process, a key requirement is the need to execute a series of tasks in a specific order. Think for a moment about the overall process involved in updating the Internet-facing firewall to allow https traffic flow to a new set of point-of-sale Web servers:

1. Access the firewall device and complete a backup task to the centralized database.
2. Create a new Network Address Translation (NAT) rule for each Web server.
3. Create a new access rule for the https traffic flow from the source outside address to the destination NAT address for each Web server.
4. Complete the manual process of testing https access to the Web servers to validate the change.
5. Commit the configuration change to NVRAM once validated.
6. Complete a second-versioned backup task to the centralized database.
7. Complete manual notification to the application manager for the point-of-sale system that the change is complete.

As you follow the required steps for a simple firewall change, you begin to see the need to apply controlled script execution throughout the automated configuration change. Each of the steps or tasks described has to be executed in the proper order. It is also important that the success of each task is monitored to ensure the overall configuration process is halted if a critical step is not completed—such as the initial backup task. An additional element to consider is the inclusion of manual tasks within the automated process. These manual tasks help to ensure external testing and notification processes are not overlooked. Scripted tasks in conjunction with the automated scheduling of configuration updates is a powerful tool and should be part of any smart network management system.

Make the Move to Smart Configuration and Change Management

SMBs often lack a full-time network configuration manager. It is not unusual for the role of "network manager" to be added to an employee's real title and responsibilities—as in President/Network Manager, Sales Rep/Network Manager, or Administrative Assistant/Network Manager.

Regardless of the size, businesses need networks that operate 24/7, providing secure and reliable access to resources, applications, and data required to function. Unfortunately, many network managers do not have the time to properly plan or execute configuration changes, and ad-hoc configuration changes usually translate into network outages.

Change the way your business approaches network management by evaluating the use of a fully integrated configuration and change management system. With the power of centralization, all device configuration data and access information is secure and readily available for recovery. Through the process of automation, major network upgrades or configuration changes can be made with confidence and completed on time. Network outage by human error is greatly reduced by scripted execution of configuration changes across multiple devices.

In a competitive environment, alignment with industry compliance standards can help to differentiate your business from competitors. An integrated configuration and change management system provides full auditing and logging of all device configuration changes helping to ensure your business stays in compliance.

Your network is growing and changing along with your business. As the network becomes more complex, the manual process of configuration and change management breaks down. Shouldn't your network management capabilities grow along with your network? Take a step in the right direction by moving your business into an integrated configuration and change management solution powered by a smart network management system.

Download Additional Books from Realtime Nexus!