Network Configuration and Change Management Software Selection For Company XYZ

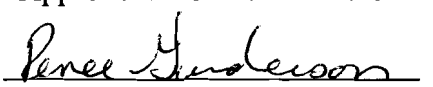
by

Todd Martin

A Research Paper
Submitted in Partial Fulfillment of the
Requirements for the
Master of Science Degree
in

Management Technology

Approved: 4 Semester Credits



Renee Gunderson

The Graduate School

University of Wisconsin-Stout

May, 2006

The Graduate School

University of Wisconsin-Stout

Menomonie, WI

Author: **Martin, Todd E.**

Title: ***Network Configuration and Change Management Software Selection for Company XYZ***

Graduate Degree/ Major: MS Management Technology

Research Adviser: Renee Gunderson

Month/Year: May, 2006

Number of Pages: 78

Style Manual Used: American Psychological Association, 5th edition

ABSTRACT

Due to security reasons and confidentiality the company will be referred to as Company XYZ. Company XYZ is a company with a data communications network of approximately 12,000 Cisco routers and switches. The Network Operations and Engineering Services department use CiscoWorks to manage and support the configurations of each of these devices. CiscoWorks is a network configuration and change management (NCCM) software suite from Cisco that is used by various users to accomplish daily tasks. These tasks include switch port and router configurations, IOS upgrades, standards verification, and various other configuration updates. CiscoWorks also backs up current running configurations to be used if there is a hardware failure and the router or switch needs to be replaced. The previous example is used to signify the importance of a network

configuration and change management tool with a network of this size. It would be a very difficult task to try and save and file configurations for 12,000 devices.

Company XYZ's Network Operations and Engineering Service department will need to select a new software tool since their current version of CiscoWorks will not be supported in a year. This paper will identify Company XYZ's use of CiscoWorks and compare viable solutions for CiscoWorks replacement that will best meet Company XYZ's needs. Possible solutions are AlterPoint's Device Authority Suite, Emprisa E-NetAware , Opsaware Network Automation, and Voyence Control NG, as well as an upgraded version of CiscoWorks.

The Graduate School

University of Wisconsin Stout

Menomonie, WI

Acknowledgments

There are a few people that I would like to thank for their encouragement and support during the process of completing this paper. I would like to thank my wife for her understanding and patience during my graduate school experience. My parents for believing in me and knowing I can accomplish goals when I set my mind on them. I would also like to thank my advisor, Renee Gunderson and my manager at Company XYZ for their guidance during this project.

TABLE OF CONTENTS

List of Tables

Chapter I: Introduction

Statement of the Problem

Company XYZ's current Network Configuration and Change Management software tool will no longer be supported by the vendor in a year.

Purpose of the Study

The purpose of this study is to identify issues relating to Company XYZ's current network configuration and change management software tool and assist in the selection of an alternative solution. There are approximately 12,000 Cisco routers and switches in their current data communications network. Network availability is critical to the business therefore these devices are important to the financial success of Company XYZ. The network configuration and change management software tool is used for tasks such as, device backup and recovery, IOS upgrades, and configuration changes. The new software tool needs to address the following goals:

- Automate changes and reduce technician direct involvement to complete tasks.
- Increase network uptime and stability.
- Compliance validation and enforcement.
- Enforce network security.

Assumptions of the Study

Assumptions of this study are as follows:

1. Company XYZ's Network Operations and Engineering Services department is using a network and configuration change management software tool, CiscoWorks for daily support and change management functions.

2. Company XYZ's current version of CiscoWorks will no longer have vendor support in one year. An updated version of CiscoWorks or a new software tool needs to be selected and implemented before that support expires.
3. Network configuration changes are part of the support process for business.

Definition of Terms

The following definitions were used in writing this research paper.

Access control list (ACL): Router configuration used to permit or deny users to services on the network (Newton, p. 41).

AlterPoint: An Austin, Texas based company that offers software products and solutions for network configuration and change management.

Change Management: A methodology for making and keeping track of changes (Ciampa, p. 507).

Cisco: A San Jose, California based company that manufactures network equipment, such as, routers and switches.

Cisco Info Center: Cisco Info Center provides a high-performance, distributed, and integrated client-server system for alarm and event management from diverse sources, including many different vendor products and standard management platforms (Cisco Info Center).

CiscoWorks: Cisco Systems software tool used for Network Configuration Management.

Configuration Management: One of five categories of network management defined by the ISO. Configuration management is the process of adding, deleting

and modifying connections, addresses and topologies within a network (Newton, p. 210).

Emprisa Networks: A Fairfax, Virginia based company that offers software products and solutions for network configuration and change management.

Firefox: Mozilla web browser.

Gramm-Leach-Bliley Act (GLBA): A federal act that requires private data to be protected by banks and other financial institutions. (Ciampa, p. 510)

Internet Explorer: Microsoft web browser.

IOS: Internetwork Operating System from Cisco. This is a outers and switch operating system (Newton, p. 450)

IP Security (IPSec): A set of protocols developed to support the secure exchange of packets (Ciampa, p. 512).

Netscape: Netscape web browser.

Network Control Center: A department at Company XYZ responsible for monitoring and first level trouble shooting network related issues.

Network Engineering: A department at Company XYZ responsible for working with internal and external customers to design and request network changes.

Network Quality Assurance: A department at Company XYZ responsible for validation and verification of network changes. Also responsible for approving and implementing network standards, such as, IOS upgrades, router and switch configurations.

Network Operations Support Services: A department at Company XYZ responsible for supporting network software tools, such as, CiscoWorks.

Network Support: Department at Company XYZ responsible for second level trouble shooting and implementing router and switch configuration changes.

Operating System: An operating system is a software program which manages the basic operations of a computer system (Newton, p. 609).

Opsware: A Sunnyvale, California based company that offers software products and solutions for network configuration and change management.

Role Based Access Control (RBAC): An access control model in which permissions are assigned to a position or role (Ciampa, p. 516).

Router: A network-layer mechanism, either software or hardware, using one or more metrics to decide on the best path to use for transmission of network traffic. Sending packets between networks by routers is based on the information provided on network layers. Historically, this device has sometimes been called a gateway (Lammle, p. 730).

Sarbanes-Oxley: A federal act that enforces reporting requirements and internal controls on electronic financial reporting systems. (Ciampa, p. 516)

Switch: In networking, a device responsible for multiple functions such as filtering, flooding, and sending frames. It works using the destination address of individual frames. Switches operate at the Data Link layer of the OSI model. (Lammel, p.739).

Terminal Access Control Access Control System (TACACS+): An industry standard protocol specification that forwards username and password information to a centralized server (Ciampa, p. 518).

Voyence: A Richardson, Texas based company that offers software products and solutions for network compliance, configuration and change management.

Limitations of the Study

Limitations to this research project are as follows:

1. This research study is for Company XYZ. The researcher is limited to network configuration and change management issues affecting only Company XYZ.
2. This research does not explain how to install and support the software for network configuration and change management. This research will compare available options that will meet Company XYZ current and future needs.
3. This research does not test the software options. Due to the availability for vendors to provide demonstrations on Company XYZ's network infrastructure.
4. The NCCM vendors will need to be brought into Company XYZ to do their own evaluation of the company infrastructure. At that time, they will provide a detailed proposal to company XYZ, detailing unanswered questions. The researcher was limited for this initial product comparison with public knowledge which is available on the various NCCM vendors' websites.

Methodology

A survey was distributed to a selection of employees in Company XYZ Network Operations and Engineering Services organization. The employees selected have various roles within the organization. Employees selected for survey came from the following departments:

- Network Control Center
- Network Support
- Network Quality Assurance
- Network Engineering
- Network Operations Support Services

The researcher also conducted an analysis of the current network configuration and change management tool, CiscoWorks, identifying hardware issues, software issues, and what other support functions that Company XYZ is using this tool for.

Due to security reasons, no vendor software was installed and ran on Company XYZ's network infrastructure. The analysis of these vendors is based on data gathered from their websites, due the limitation of them disclosing confidential and proprietary information without their evaluation and proposal to Company XYZ. Network configuration and change management tools are not "buy off the shelf and install" products that can be implemented into a company's network management solution. Variations in different company's needs are: number of devices, make and model types, versions of IOS or operating systems, reports that are needed, and add-in software applications that are used by the company.

Chapter II: Literature Review

Introduction

The review of the literature presents information for a companies need to use a network configuration and change management solution to assist in daily tasks to ensure network availability and to accomplish new changes to the enterprise network. A network configuration and change management solution can be used for several tasks and processes within a Network Operations Center. Those tasks include automating router and switch configurations, IOS upgrades, and backup of device configurations. Compliance validation and audit control as it pertains to various government requirements, such as Sarbanes-Oxley Act, and the Gramm-Leach-Bliley Act. Improving and enforcing network security by restricting unauthorized users is critical to business operations.

Types of Network Changes

Many people have different definitions of the term network. For the purpose of this research, a network device will be defined as a device that moves data along to its intended destination. The device can also be used to block or restrict traffic if it is not intended for that path. Primary focus for this literature review will be routers and switches.

Networks can be used by internal and external customers for access to e-mail servers, file transmissions, e-commerce activities, along with other business functions. There can be numerous network changes daily that leads to the financial success of a company. Examples of network changes are as follows:

- Host router interface configuration for a new remote site.

- Switch port activation for a new server. Switch port deactivation for a no longer needed server.
- Password changes on devices.
- Access-List statements for permitting or denying users to the network.
- Replacing a non-functioning router or switch. IOS and configurations need to be added to the replacement device.

Change Management

What is Change Management? Change Management is a methodology for making and keeping track of changes (Ciampa, p. 507). Network change management is the process and tool of implementing the various configuration changes that are needed to meet internal and external customer requests. These changes need to be documented and scheduled accordingly to ensure the least impact or disruption on the business. The object of change management is to ensure standardized methods and procedures are used for efficient and prompt handling of changes, in order to minimize the impact of any related incidents upon completion.

Configuration Management

What is configuration management? Configuration management is one of five categories of network management defined by the International Standards Organization. Configuration management is the process of adding, deleting and modifying connections, addresses and topologies within a network (Newton, p. 210). Colville (2006) suggests that a Configuration Management Database (CMDB) should address the following four functions:

1. Reconciliation - The CMDB is able to distinguish the same device from various sources. The discovery tool will recognize the device by IP address, hostname, or MAC address, but the CMDB will only create one configuration for that device. This avoids any duplicate devices within the CMDB.
2. Federation. – This allows for multiple data sources to be linked. Used to verify configurations from various sources to be compared to each other.
3. Mapping and visualization – This provides the ability to illustrate logically or physically the peer-to-peer and hierarchical relationships between the configuration items.
4. Synchronization – This it the ability to update the CMDB with approved changes, and identify changes that are not approved. If an unapproved change is detected, it will send a notification trigger to the appropriate IT department to investigate and potentially revert to the previous device configuration.

Manual Changes vs. Automation

Manual configuration of routers and switches is a time consuming process, for example, an access-list configuration can be hundreds of lines. This configuration change is implemented by the technician typing line by line the needed commands to make the change. This tedious task allows for a chance for human error. According to Dubie (2004), the Yankee Group survey of 229 network operators found human error to be the second-largest cause of outages. Telco or Internet Service Providers (ISPs) counting for 35%, followed closely by human error 31%, with power failure, hardware failure and unresolved problems also listed as reasons. Taylor and Metzler (2005) have reported estimates up to 60% of both enterprise and service-provider network outages involve

human error of some sort. The errors could be from incorrectly configured equipment to incompatible software releases. By automating change and configuration tasks it will allow many devices to be updated at one time and reduce the chance of mistyping a command. There is also a need to have a backup copy of the configuration saved on the network, so reverting to the previous configuration or IOS version is available.

Compliance and Audit Control

One change in the corporate world has been compliance and audit control due to recent scandals such as Enron and Worldcom. The government has introduced several acts and regulations over the years to protect investors and customers of a company, for example Sarbanes-Oxley and Gramm-Leach-Bliley. There are auditing processes and change management controls that are important considerations for company's information technology department. Records of change and standards are needed for internal and external auditing. There is also a need to have security controls in place. Companies need to document internal network topologies and IOS standards for external auditors to verify there is not a security risk.

Security

Security is more then the fence, lift gate, and badge readers in and around the building. Security is a critical part of the information technology (IT) department responsibility. The IT department needs to know who is logging into the network devices and who has permissions to make changes to the network devices. There is a need to control who has access to the network, internal and external users. One method to control who is logging into a system is the use of a TACACS+ login. TACACS+ is an industry

standard protocol specification that forwards username and password information to a centralized server (Ciampa, p. 235).

Role Based Access Control (RBAC) is another why to secure the network from internal staff. RBAC is assigning privileges or rights to individuals based on their function within the organization. Network departments often use this to assign rights to users such as, read only rights, what devices can users log into, and what changes they can make.

CiscoWorks LAN Management Solution 2.2

CiscoWorks LAN Management Solution 2.2 is an application suite that is used for configuring, monitoring, and trouble shooting Cisco networks. The following are applications that are included as found on the CiscoWorks LAN Management Solution 2.2 Introduction website:

- CiscoWorks Campus Manager
- CiscoWorks Devcie Fault Manger
- nGenius Real-Time Monitor
- CiscoWorks Resource Manager Essentials
- CiscoView
- CiscoWorks Mangement Server

The application that is most used in regards to CiscoWorks configuration and change management is CiscoWorks Resource Mangers Essentials. Cisco RME is used for inventory and change management, network configuration, software image management, network availability, and syslog analysis.

The following are End-of-Sale and End-of-Life milestone dates regarding CiscoWorks LAN Management Solution 2.2 as found on Cisco's End-of-Life and End-of-Sale Notice website:

- January 31, 2005 – End-of-Life Announcement Date. This date was to announce the end of sale and end of life of the product to the general public.
- July 31, 2005 – End-of-Sale Date. This was the last date the product was available for sale.
- October 31, 2005. Last Shipment Date. This was the last ship date that Cisco or its contracted manufacturers could ship product.
- July 31, 2006. End of Software Maintenance Release Date. This is the last date that Cisco Engineering may release any final software maintenance releases or bug fixes. After this date, Cisco Engineering will no longer develop, repair, maintain, or test the product software.
- July 31, 2006. End of New Service Attachment Date. This date is for equipment and software that is not covered by a service-and-support contract, this is the last date to order new service-and-support contract or add the equipment and/or software to an existing service-and-support contract.
- July 31, 2007. End of Service Contract Renewal Date. This date is the last date to extend or renew the service contract fro the product. The extension or renewal period can not extend beyond the last date of support.
- July 31, 2008. Last Date of Support. This is the last date to receive service and support for the product. After this date, all support services for the product are unavailable, and the product becomes obsolete.

NCCM Solutions Available

There are a few solutions available to accommodate and support a large enterprise network configuration and change management needs. Those solutions are AlterPoint Device Authority, Emprisa E-NetAware, Opsware Network Automation System, Voyence Control NG, and upgrading to the latest version of CiscoWorks LAN Management Solution 2.5.1. These solutions focus on change and configuration automation, audit and compliance, and security.

Chapter III: Methodology

Statement of the Problem

Company XYZ's current Network Configuration and Change Management software tool will no longer be supported by the vendor in one year.

This chapter will be used to select and identify Company XYZ's Network Operations and Engineering Services department support staff that uses CiscoWorks to complete their assigned roles within the organization. A survey of 13 questions was e-mailed to staff members identified that have used CiscoWorks since January 1, 2006. Topics covered in this chapter include, subject selection and description, instrumentation, data collection procedures, data analysis, and limitations.

Subject Selection and Description

Company XYZ's Network Operations and Engineering Services organization has several departments that rely on the use of the network configuration and change management tool, currently that is CiscoWorks LAN Management Solution 2.2. The various departments use the tool to complete tasks related to their role within the organization. CiscoWorks administrators have defined the following roles and responsibilities:

1. Network Administrator: Configuration and IOS Administration
2. Approver: Job approval for configuration changes.
3. Network Operator: Job review of configuration changes.
4. Help Desk: View only reports and check device inventory.
5. Export Data: Exporting Inventory Data.
6. Developer: Process Administration.

The people assigned to the various groups in CiscoWorks were used to collect information on strengths, weaknesses, and limitation issues pertaining to their use of the tool.

The following have been selected as potential replacements to CiscoWorks at Company XYZ, AlterPoint Device Authority Suite, Emprisa E-NetAware, Opsware Network Automation Suite, and Voyence Control NG. There is also an updated version of CiscoWorks, CiscoWorks LAN Management Solution 2.5.1. There will be an initial comparison of these products, to determine if they may meet Company XYZ's requirements as a replacement to CiscoWorks LAN Management Solution 2.2.

Instrumentation

The following instruments were used to collect data:

1. A survey was e-mailed to users within Company XYZ Network Operations and Engineering Services organization. The survey was created to identify current uses and identify any issues of CiscoWorks at Company XYZ.
2. Information was gathered from potential replacement solutions to CiscoWorks from their respective websites.

Data Collection Procedures

A 13 question survey was administered to 20 Company XYZ Network Operations and Engineering Services staff members in various roles across the organization. The staff members were selected from 40 users that have login IDs to the CiscoWorks servers. The selection of the 20 participants were decided on recent login activity on the servers, this is to identify any current issues they were having since January 1, 2006.

Data Analysis

The survey was intended to identify issues that current users of CiscoWorks are experiencing. The survey was used to identify time it takes to create and run CiscoWorks Netconfig or Distribute by Device jobs. As well as identify any reports that are currently being run.

Limitations

Due to proprietary and confidential information and the replacement vendor's requirement to complete their own analysis of Company XYZ, the research is limited to public knowledge information available on the vendor's website.

Chapter IV: Results

Introduction

The purpose of this study was assist in the selection of replacement Network Configuration and Change Management solution for Company XYZ's current tool CiscoWorks LAN Management Solution 2.2. Cisco Systems has announced that this version is at the End-of-Life. Company XYZ will need to purchase an upgrade version of CiscoWorks or purchase a potential replacement solution.

Company XYZ Introduction

Due to security reasons and confidentiality the company will be referred to as Company XYZ. The network infrastructure is very important to this company to ensure financial success. Therefore, no individuals, IP addresses, DNS names, or physical building locations will be identified in this research.

Company XYZ has numerous devices on their network. The following is a list of device examples:

- Cisco routers
- Cisco switches
- 3Com switches
- Bay/Nortel switches
- Synoptics Hubs
- F5 Load Balancer
- Firewalls
- Microsoft Windows Servers
- Unix Servers

This research is looking at the network configuration and change management tool for routers and switches, CiscoWorks, the departments that use CiscoWorks, and a potential replacement. The following departments within Company XYZ's Network Operations and Engineering Services have been identified as CiscoWorks users in some capacity:

- Network Control Center
- Network Support
- Network Engineering
- Network Quality Assurance
- Network Operations Systems Support

Besides CiscoWorks, Company XYZ uses the following tools to detect, manage and track trouble incidents, change management, and problem records. BMC Remedy Action Request System is used for incidents created by the Network Control Center when there is network change event that triggers a Cisco Information Center (CIC) event. The event typically is a topology change due to a change in the network status. Examples of events could be a duplex mismatch, HSRP issue, host interface or port down status. Network Engineering and Network Support typically create change management records in BMC Remedy Action Request System to generate an electronic trail of network changes that will be created in CiscoWorks. A problem record would be created by Network Quality Assurance or Network Engineering when it has been identified by Cisco and Network Support that there is a bug in a particular IOS version and an upgrade will be required on all Company XYZ devices of that platform. Peregrine AssetCenter is used as a database for Company XYZ to document information about sites, such as, street

address information, contact information, IP addresses, DNS names, equipment types, and serial numbers for sites on the network.

CiscoWorks Overview at Company XYZ

Company XYZ currently uses CiscoWorks LAN Management Solution 2.2 for managing approximately 12,000 Cisco devices. Model types range from 1700 series routers, 2600 series routers, 2950 switches, and 6509 switches, along with others. Figure 4.1 shows the breakdown of each server and the number of Cisco devices managed on each.

Table 4.1 Number of Cisco Devices Managed By Each CiscoWorks Server

Server	Number of Devices
CiscoWorks Server 1	1,837
CiscoWorks Server 2	1,837
CiscoWorks Server 3	1,863
CiscoWorks Server 4	1,138
CiscoWorks Server 5	1,319
CiscoWorks Server 6	1,772
CiscoWorks Server 7	2,109
Total	11,875

The following is the CiscoWorks Server information at Company XYZ.

Make: Sun Microsystems

Type: 220R

Model: Fire V250

Operating System: Solaris

Version: G117350-04

Release : 5.8

Physical RAM: 2048 MB

The following is a workstation configuration that is used by Company XYZ's Network Operations and Engineering Services department:

System: Microsoft Windows XP Professional Version 2002 Service Pack 1

Computer: Intel Pentium IV 2.80 GHz 1.25 GB of RAM

Browser: Internet Explorer version 6

What is CiscoWorks being used for at Company XYZ? The Network Operations and Engineering Services use CiscoWorks for various daily tasks to schedule and manage configuration changes. CiscoWorks Netconfig is used to create and schedule a network change job for a router or switch. There then is a CiscoWorks Approver function that is used to initiate job at the appropriate scheduled time. CiscoWorks is also used to retrieve the previous known configuration when a hardware replacement is needed. Reports are also generated from CiscoWorks to compare device configurations to Company XYZ's established standards.

Company XYZ CiscoWorks Survey Results

There are 40 users identified by Company XYZ CiscoWorks Administrators that have logins to CiscoWorks for various roles and responsibilities within the Network Engineering and Operations Services. The roles and responsibilities are as follows:

1. Network Administrator: Configuration and IOS Administration.
2. Approver: Job approval for configuration changes.
3. Network Operator: Job review of configuration changes.
4. Help Desk: View only reports and check device inventory.
5. Export Data: Exporting Inventory Data.
6. Developer: Process Administration.

There were 20 people identified that have used CiscoWorks since January 1, 2006. These users were e-mailed CiscoWorks Survey that is in Appendix A. The following were the results:

Number of Surveys Sent: 20

Number of Surveys Returned: 16

Question 1. Do you use CiscoWorks?

All 16 responses do use CiscoWorks in some capacity to complete their assigned role within Network Operations and Engineering Services organization at Company XYZ.

Question 2. How often do you use CiscoWorks?

The following were the results of how often they use CiscoWorks.

Table 4.2 Frequency of using CiscoWorks

Frequency	Number of Users
Daily	50 %
2-4 Times/Week	25 %
2-4 Times/Month	12.5 %
2-4 Times/Year	12.5 %

Question 3. What do you use CiscoWorks for?

CiscoWorks can be used for variety of tasks to complete configuration changes and other tasks. The following were the responses from the survey participants:

Table 4.3 Company XYZ use of CiscoWorks

Task	Number of Users
Information Only	5
Device Inventory	11
IOS Upgrades	11
Configuration Backup	7
Port Activations	10
Interface Configurations	10
Access List Configurations	8
IPSec Configurations	4
Netconfig or DBD Job Approver	8

Question 4. How long does it take you to create CiscoWorks configuration job?

There is a variation in time it takes for Netconfig Job creators to build their configuration change. The results are shown in table 4.4 CiscoWorks Netconfig Job Creation Time.

Table 4.4 CiscoWorks Netconfig Job Creation Time

Time	Percent of users
1 minute	10%
2 minutes	20 %
5 minutes	30 %
10 minutes	30 %
30 minutes	10 %

The reasons for the variation in time to create jobs could depend on a few factors, such as, what is the type of configuration change, is it a few lines or is it several lines as in an access list configuration. The more lines, the more time it will take to type the needed lines into the configuration. Training or lack there of, in CiscoWorks or repetition of job creation may also be reasons for the differences in time.

Question 5. Has your CiscoWorks job failed?

This questions was intended to find out if the CiscoWorks job creator had a change job that failed. Of the five people that responded, four had jobs that failed, one reported that they had not had a job fail. If jobs have a failed status, it is up to Network Support to verify and resolve any issues, many times when a job fails, this results in Network Support completing the configuration change manually. To complete the configuration task manually, can be a time consuming event, if the job had multiple routers or switch changes.

Question 6. If your CiscoWorks job failed, please indicate issue/reason for failure.

Asking this question on the survey was to identify what reasons CiscoWorks jobs

failed. Was it user error, server error, syntax issue, or something else? The following were reasons from the survey respondents:

- Syntax errors. This is when the CiscoWorks Job creator, types in incorrect or incomplete Cisco command and it is not recognized by the router or switch.
- Operator error. This is the result of Network Support (Job Approver) not approving the job in time.
- More then one job set to run to a device at the same time.
- Jobs fail to sync to Archive. This means that after job ran, it does not save the configuration to the server for a recent backup copy of the configuration.
- Server issue. Rare occasion, but a non responsive server, the change configuration jobs need to be run manually.

Question 7. If you use CiscoWorks for IOS upgrades, how long does it take to complete?

Knowing that Company XYZ has different bandwidths to the various sites, this question was used to try and determine about how long it takes to complete an IOS upgrade. A Cisco IOS is the code that is used as the operating system of the router or switch. Results were between 20 minutes and 90 minutes. An example would be a Cisco 2600 series router would take forty five minutes over a 128K circuit. Another example would be a 2800 series router, with an IOS less then 32 MB, could take up to 90 minutes.

With Company XYZ's current CiscoWorks server version and configuration, circuit speeds, and other variables, during IOS upgrades, it has been found that it is best to run twelve jobs, with twelve devices per job at a time. This takes about three hours to complete. This can be a very time consuming to upgrades hundreds of devices.

Question 8. If you use CiscoWorks to run any reports, what type of reports and what is the report used for?

With acts such as, Sarbanes-Oxley and Gramm-Leach-Bliley, there has been more government regulation and requirements to implement audit and compliance controls at organizations. The survey found that the following reports are being generated at Company XYZ:

- Software Report/Software Version Graph. This report is being used to identify what devices are running the current approved IOS image.
- Search Archive by Device/Search Archive by Pattern. Used to verify current running configurations.
- Change Audit. Verify change have been made and by whom.
- Hardware Report/Chassis Summary Graph. Determine which platforms are currently in CiscoWorks. It is used to create static views of platforms based on Company XYZ published standards. Also used when doing IOS upgrades to determine if the platforms have the minimum memory and flash required for a specified IOS.

Question 9. Do you create CiscoWorks Jobs to back out of changes? Or do you rely on manual back out procedures?

It is found that most, Netconfig job creators rely on manual back out procedures. A back out procedure would be to return the router or switch to the previous configuration if determine there is an end device issue or error, the new configuration is causing a network outage, or is no longer needed. Company XYZ Change Management

department and procedures allows for job requesters to document the back out procedures in the Change Management Record in the BMC Remedy Action Request System.

Question 10. How long did it take you to create the back out job?

For the few requesters that do create back out jobs, it is found that it can take about five to ten minutes to create that job. In cases of large configuration change, multiple router changes, it can take up to thirty minutes to build the back out job. Most Cisco configuration changes can be backed out by adding a "no" in front of the requested change configuration commands.

Question 11. How long does it take on average to back out of change?

Once determined that the configuration change is either causing an outage or no longer needed, it can take about ten minutes to back out of the change.

Question 12. Would you like to use a software program that allows you to revert to previous configuration?

Some network configuration and change management solutions have an option built in, that allows the configuration to be reverted to the previous configuration. This can be very useful instead of going through a manual process of typing in the back out procedures or taking the time to create a back out job. Twelve respondents to the survey stated that they would like this option.

Question 13. Any additional comments/issues/limitations you would like to make about using CiscoWorks.

This open ended question was an opportunity for CiscoWorks users to add any additional comments, issues, or limitations that they have experienced with CiscoWorks. The following are some of the responses:

- One of the biggest limitations of CiscoWorks is that a company of Company XYZ size, you are unable to manage a network of 12,000 devices on one server. There is a need to have multiple servers, which increases administration efforts.
- Difficult at times to determine why Netconfig or Distribute by Device job fails. Occasionally there is no explanation. Cisco's explanation often associates failure with a bug that will be fixed in a future release.
- Global changes can be very time consuming to create. An example would be changing the passwords on all the routers and switches. It would take over 100 CiscoWorks jobs across seven different servers. The reason for this many jobs is because you need to create a separate job for 1900 series switch, IOS based, and Catalyst devices. During this job creation, there is need to limit number of devices due to time constraints. There is also a need for a second job to be created to verify that the change was complete. Then the job implementer needs to go thru the job status and address any errors that may have occurred. This process can be a long, labor intensive and tedious process.
- CiscoWorks does not accurately report if devices are currently responding. This causes issues if there is a global change. This can increase the number of failures to sort thru during the verification process, which can take several hours.
- Company XYZ has not added all the applications available with Cisco Resource Manager Essentials 3.5, such as "Reload History" and Campus Manger".
- Company XYZ has found with their current server configuration that there is a limit of 2,500 devices per server.

- The Internet Explorer user interface is slow and takes several minutes at times to refresh screen. This is a time consuming process when the job approver has 30 jobs to approve for one nights change window. Each job needs to be approved separately, and the screen needs to refresh between each approval.
- Issues of slow response could be addressed with upgrading the CiscoWorks servers.

NetConfig and Distribute by Device Analysis

The following tables are a historical analysis of Company XYZ Netconfig and Distribute by Device jobs for the first three months of 2006. Netconfig jobs are used for daily change configurations such as; host router interface configurations and switch port activations. This will also show that CiscoWorks is used for hundreds of network changes per month.

Table 4.5 CiscoWorks Netconfig Jobs January 2006

Netconfig Status	CiscoWorks 1	CiscoWorks 2	CiscoWorks 3	CiscoWorks 4	CiscoWorks 5	CiscoWorks 6	CiscoWorks 7	Totals
Number of Devices	1837	1837	1863	1138	1319	1772	2109	11875
Succeeded	21	20	20	26	0	63	29	179
Failed	18	7	14	10	0	46	44	139
Rejected	16	17	8	7	0	21	34	103
January Netconfig Jobs	55	44	42	43	0	130	107	421

Table 4.6 CiscoWorks Netconfig Jobs February 2006

Netconfig Status	CiscoWorks 1	CiscoWorks 2	CiscoWorks 3	CiscoWorks 4	CiscoWorks 5	CiscoWorks 6	CiscoWorks 7	Totals
Number of Devices	1837	1837	1863	1138	1319	1772	2109	11875
Succeeded	12	21	7	21	65	72	23	221
Failed	5	2	2	4	5	9	10	37
Rejected	3	1	2	6	15	9	8	44
February Netconfig Jobs	20	24	11	31	85	90	41	302

Table 4.7 CiscoWorks Netconfig Jobs March 2006

Netconfig Status	CiscoWorks 1	CiscoWorks 2	CiscoWorks 3	CiscoWorks 4	CiscoWorks 5	CiscoWorks 6	CiscoWorks 7	Totals
Number of Devices	1837	1837	1863	1138	1319	1772	2109	11875
Succeeded	8	15	14	9	224	152	25	447
Failed	4	7	8	4	17	26	4	70
Rejected	0	5	3	1	29	19	6	63
March Netconfig Jobs	12	27	25	14	270	197	35	580

During the first three months of 2006, there were 1,300 Netconfig jobs created. The succeeded job status was for jobs that were completed and had no issues or errors. The failed status required Network Support to manually verify what part of the configuration change error, rerun the job or type the configuration into the router or switch. The reasons for failure could be syntax issue, more then one job running to a device at a time, device unreachable, or could not initiate a ssh session. The rejected status is for jobs that were created, usually it was a back out job that was not approved and is no longer needed.

Distribute by Device jobs are used to upgrade Cisco IOS on routers and switches. An IOS upgrade is used to update the operating system on a router or switch. Reasons for upgrading IOS are: new features available, a bug is identified with that version of IOS, or to harden security. The following a snap shot of Company XYZ's Distribute by Device status for the month of March 2006.

Table 4.8 CiscoWorks Distribute By Device Jobs March 2006

DBD Job Status	CiscoWorks 1	CiscoWorks 2	CiscoWorks 3	CiscoWorks 4	CiscoWorks 5	CiscoWorks 6	CiscoWorks 7	Totals
Complete	100	109	101	25	14	2	0	351
Error	4	3	3	1	6	0	0	17
Reject	4	11	2	2	3	2	0	24
					Total DBD Jobs			392

The reasons for Error or Reject are similar to Netconfig, usually there is a error status when there is a timeout trying to connect to that device to start the process of upgrading the IOS. Occasionally there will be a WAN network provider or hardware

issue causing the error. A reject status is for jobs that do not get approved. This could be from either operator error by forgetting to approve or decided to reschedule the devices for upgrade at a later date.

Network Configuration and Change Management Software Vendors

There are several different vendors that develop and provide some level of Network Configuration and Change Management solutions. They vary in aspects to working for small, medium, and large enterprise organizations. AlterPoint Device Authority, Emprisa E-NetAware, Opsware Network Automation System, and Voyence Control NG have been identified as potential replacements to CiscoWorks or enhancements to Cisco Resource Management Essentials. These solutions focus on Automation, Compliance and Audit Control, and Security, which are critical concerns for Company XYZ. Other items that are being used for comparisons are server requirements, end user workstation requirements, devices supported, and third party integration with other network management tools. Due to the vendor's e-mail responses, information on licensing, cost of system, and other proprietary and other confidential information a full analysis of the tools is unavailable. Company XYZ's management team will need to contact the vendor's and request the vendors create a proposal after they asses Company XYZ's infrastructure.

AlterPoint Device Authority

AlterPoint Device Authority is a network change and configuration management tool from AlterPoint Inc. This solution focuses on change, compliance and security features for a company to manage their enterprise network. AlterPoint Device Authority supports a number of network devices, such as Cisco, 3Com switches, and Extreme

Networks. The complete list of supported devices can be viewed in Appendix F: NCCM Supported Devices. This solution provides third party integration with other network management tools, such as, BMC Remedy Action Request System, HP Openview Network Node Manager, IBM Tivoli and others. NCCM integrations can be found in Appendix I. NCCM Integrations.

The following are AlterPoint Device Authority server requirements:

Operating System (server will need to be one of the following):

- Microsoft Windows 2000/2003
- Sun Solaris 9
- Redhat Linux ES3/AS3/ES4/AS4

Hardware for Microsoft Windows/Linux server:

- 1 GHz Pentium IV
- 1 GB Memory
- 10 GB disk

Hardware for Sun Microsystems server:

- UltraSPARC III
- 2 GB Memory
- 20 GB disk

Database server (one of the following):

- MySQL v4.1.9
- Oracle 9i & 10g
- Microsoft SQL 2000

The following is AlterPoint Device Authority end user workstation requirements:

Operating System:

- Microsoft Windows 2000/2003/XP Professional

Hardware:

- Intel Pentium III 700 MHz or greater
- 512 MB Memory
- 100 MB disk

User Interface:

- Display Resolution: 1024x768 or greater
- Microsoft Internet Explorer 6 with Service Pack 1 or greater with 128-bit encryption
- Desktop Client: Integrated Network Environment (INE)

AlterPoint provides the following change management features (AlterPoint Solutions: Change):

- Automate configuration changes to multiple network devices simultaneously.
- One-click restoration (roll-back) to previously good configuration.
- Intelligent change wizards to simplify and automate complex and routine changes (passwords, SNMP community string) reducing risk of human error.
- Command syntax verification prior to deploying change.
- Feedback on success or failure of change to network infrastructure
- Validation (pre-change) or verification (post-change) to identify preventative or remedial actions.
- Peer reviews of changes being implemented

- Real-time detection of unauthorized and network change errors
- Role Based Security Access
- Notification of changes taking place on network
- Change management reports to document changes are occurring within defined parameters.

There are a few reports that AlterPoint Device Authority provides that identify changes within the network. The reports are as configuration change report, change trend report, and software change report. These can be used to identify changes that have occurred on the network.

AlterPoint Configuration Change Report provides the following information:

- IP Address of device
- Host name of the device
- Make of device
- Model number of device
- Changed date
- Configuration type
- Changed by username
- Previous configuration
- Changed configuration

AlterPoint Change Trend Report is used to graph out the number of changes done daily, weekly, and monthly. The graph shows if the change was a configuration change, software, or hardware change.

AlterPoint Software Change Report is used to identify IOS image changes. The report shows the information if the device has been upgraded or downgraded. The following information is shown in the report:

- IP Address
- Hostname
- Class
- Make
- Model
- Change date
- Previous IOS Image
- Changed IOS Images

Due to government regulation, compliance and audit control have been added to the network configuration and change management solution. AlterPoint has focused and created solutions for internal and external regulations, such as Sarbanes-Oxley, Gramm-Leach-Bliley (GLBA), and others. The complete list is located in Appendix G: NCCM Audit and Compliance Controls. AlterPoint compliance capabilities as listed from AlterPoint Solutions Area: Compliance website:

- Audit trail of all changes to network infrastructure.
- Real time detection and notification of unauthorized and change errors on the network.
- Device audits of compliance with established standards.
- Scalability to manage compliance across the entire network.
- Ensure network resilience with secure roles-based user access.

- Deploy approved and standardized changes to IT network infrastructure.

AlterPoint has a few reports relating to compliance, SOX Audit Report and Graphical Policy Summary Reports. The Graphical Policy Summary Report shows the number of devices in compliance, as well as the number of devices out of compliance.

Security is very important to protect the network infrastructure. Network risks include human errors, as well as configuration and IOS vulnerabilities. AlterPoint provides the following approaches to security (AlterPoint Solutions: Security):

- Rapid identification of exposed vulnerabilities.
- Automate IOS upgrades to mitigate vulnerabilities and bugs.
- Role Based Access Control.
- Use TACACS+, RADIUS, and two form authentication schemes such as Secure Computing Safeword.
- Device Authority is a secure application following government and financial institution guidelines.
- Provides an audit trail of all network changes.
- Encrypt data repository.
- Use secure protocols to communicate with devices (HTTPS, SSH, SCP, etc.)

Emprisa E-NetAware

Emprisa E-NetAware is a network change and configuration management tool developed by Emprisa Networks Inc. E-NetAware has 15 different devices that they currently support, as listed on their website Solutions: Multi-Vendor Networks. Devices include routers, switches, firewalls, and wireless access points. Brand names are Cisco, 3Com, Alcatel, Juniper, as well as others. The complete list of devices is located in

Appendix F: NCCM Supported Devices. Emprisa E-NetAware also has a number of third party integrations with other network management tools, Appendix I: NCCM integrations, lists the products.

Emprisa E-NetAware server requirements:

Operating System (one of the following to be used on the server):

- Microsoft Windows 2000/2003/XP Professional
- Sun Solaris 8, 9, or 10
- Linux

Hardware:

- 1 GHz Pentium III
- 1 GB Memory
- 80 GB Hardrive

Emprisa E-NetAware workstation requirements:

- 256 MB memory (recommended)/128 MB required
- Display Resolution: 800x600 resolution
- Microsoft Internet Explorer 6.x and above
- Firefox version 1.x and above
- Netscape version 7.1 and above
- Mozilla version 1.4 and above

Emprisa E-NetAware has the following approach to addressing a network configuration and change management solution. There is a central configuration repository that tracks current, trusted and historical configuration and OS image versions for each device. An end user interface Dashboard is used to identify unplanned,

unauthorized and non compliant changes. There are a number of reports that E-NetAware is capable of running, Change Summary, Change Discrepancy, Compliancy Summary, Configuration Comparison, Configuration Trends, Device Inventory, Job Summary and OS Image History reports (Emprisa – Solutions: Configuration & Change Management). Other change management functions of E-NetAware include change workflow and OS Image Management and Change Remediation.

Emprisa E-NetAware uses the following to identify network changes:

Change Summary Report:

- Date
- Severity of event caused by change
- Category
- Source of change
- Event
- Target device name
- Description of change
- Current running configuration with date and time
- Trusted configuration with date and time

From the E-Netaware Dashboard IT personnel can police and monitor change, assess impact of changes, and accept/reject changes (Emprisa Solutions: Change Remediation).

E-Netaware's OS Image Management creates is a one look interface for managing various vendors operating system upgrades. This eliminates the complexity of interfacing with variations of upgrading the various device types. There is the ability to distribute OS

images to one or more devices, rollback to previous version, audit and report changes to OS images, and maintain an OS image library (Emprisa Solutions: OS Image Management).

Compliancy is addressed in few ways with the Emprisa E-NetAware solution. There are compliancy standards, compliancy auditing, compliancy notifications, compliancy enforcement, and compliancy reports (Emprisa Solutions: Compliance Auditing & Enforcement). These are used to verify configuration and security standards to reduce outages caused by vulnerabilities.

Emprisa E-NetAware security approach has the following features as listed on the Emprisa Solutions: Security website:

- Know "Who/What/When/Where" of change. Using the E-NetAware Dashboard, there is a ability to monitor unauthorized, unplanned and non-compliant changes.
- Deploy security-related configuration changes. Security patches, password changes, access-list changes, SNMP community strings, and other needed security changes can easily be updated on devices.
- Audit and enforce compliance with security policies. Thru the use of management audits, IT personnel can address violations as detected.
- Securing NCCM operations. E-NetAware secures network changes by, user authentication, user roles, secure network communications, HTTPS, and encrypted user and device passwords.

Opsware Network Automation System

Opsware Network Automation System is a network change and configuration management suite from Opsware Inc. This application suite allows network staff to have

visibility and control over device configurations and reducing any errant configurations that cause 80% of network downtime (Opsware: Configuration Management).

Server and workstation operating and hardware requirements were not available on the Opsware Network Automation System website. This information is provided during Opsware, Inc. evaluation and sales proposal to the particular company.

Opsware has the following capabilities as found on their website Opsware Inc: Configuration Management:

- Discovery and detailed inventory. Collecting detailed information about the network devices. Information includes: device manufacturer, model, OS version, patch level, and configuration.
- Real-time change detection. Identifies and records configuration changes. Notifications are sent to network staff to provide visibility to planned, unplanned, and unauthorized changes.
- Policy-based and ad hoc rollback. The ability to revert to previous configuration if determined new configuration is unauthorized or causing an issue.

Opsware Network Automation System offers an interface for IT personnel to access various reports for regulatory compliance. Capabilities are: centralized policy management, built in best practices, automatic enforcement and compliance reporting (Opsware: Compliance Management). A list of audit and compliance regulations for Opsware is included in Appendix G: NCCM Audit and Compliance Controls.

An optional subscription for Opsware Network Automation System is Opsware Network. This subscription has the following security features; actionable alerts, rapid remediation, and historical alerts. Actionable alerts are vulnerability notifications that are

packaged and uploaded onto the Opsware Network website in form of compliance polices. Once on the Opware Network Automation System, network staff can run compliance checks to vulnerable devices. Historical alerts allow network staff to view vulnerabilities for the past 13 years to ensure that your network devices are not exposed for all supported vendor platforms (Opsware: The Opsware Network for NAS).

Network Visualization is another feature of Opsware Network Automation System. This is a tool that maps Layer 2 and Layer 3 network to enable a deeper understanding of the entire network, and allows for swifter and accurate troubleshooting. Visual analysis has the following unique benefits: Proactively identify devices and servers that will be impacted by change, gain immediate and accurate insight into network relationships when troubleshooting, and eliminate the laborious manual process of creating network diagrams (Opsware, Network Visualization).

Voyence Control NG

Voyence Control NG is a network configuration and change management solution from Voyence Inc. Their product is focused on change automation, compliance and security. Certified devices range from routers, switches, load balancers, and others. The full list of devices can be viewed in Appendix F: NCCM Supported Devices.

Voyence Control servers and workstation requirements provided on the Voyence Control NG website are as follows:

Application Server Requirements

Operarting System:

- Sun Solaris 9
- Red Hat Linux ES3/AS3

Database:

- Postgres SQL

Linux Hardware (minimum per instance):

- Processor: Intel P4 2 GHz
- Memory: 2 GB
- Two ATA/SATA 40 GB 7200 RPM drives

Solaris Hardware (minimum per instance):

- Processor: V210 UltraSPARC 1 GHz
- Memory: 2 GB
- UltraSCSI two 146 GB 7200 RPM drives

Device Server Requirements:

Linux Hardware (minimum per instance):

- Processor: Intel P4 2 GHz
- Memory: 2 GB
- Two ATA/SATA 40 GB 7200 RPM drives

Solaris Hardware (minimum per instance):

- Processor: V210 UltraSPARC 1 GHz
- Memory: 2 GB
- UltraSCSI two 146 GB 7200 RPM drives

Client Requirements:

- Windows 2000 or XP Operating System
- Processor: 600 MHz
- Memory: 256 MB

- Non-Volatile Storage: 25 MB
- Browser Microsoft Internet Explorer 6.0/Netscape 6.0+/Firefox 1.0

A few change management benefits Voyence Control NG website lists as benefits:

- Use "Golden Configs" to create templates for new device deployments.
- Automate commonly-executed IT network management tasks in fraction of the time
- Meet the ideal frequency of credential, ACL, and OS updates for your entire network.
- Eliminate standard change errors.

Voyence Control NG offers customized solutions for Sarbanes Oxley, Gramm-Leach-Bliley and others. Compliance reports are available to use to avoid penalties.

Voyence Control has features that allow you to respond to vulnerabilities and respond to security risks quickly. Deploy security-related updates in minutes per network, versus minutes per device (Voyence Control NG).

Some examples of Voyence Control NG capabilities as found on the Voyence Control datasheet. In less then 120 minutes, you can:

- Roll out passwords and SNMP credentials for 5,000 devices
- Update operating system images over 100 devices
- Respond to a virus by modifying Access Control Lists on 5,000 devices
- Audit 15,000 devices for compliance
- Remediate non-conmpliant configurations on over 1,000 devices.

CiscoWorks LAN Management Solution 2.5.1

CiscoWorks LAN Management Solution 2.5.1 is a network configuration and change management solution for Cisco networks. According to the website for CiscoWorks LAN Management Solution 2.5.1 the following are included:

- CiscoWorks Device Fault Manager (DFM) 2.0.3
- CiscoWorks Campus Manager 4.0.3
- CiscoWorks Resource Manager Essential (RME) 4.0.3
- CiscoWorks Internetwork Performance Monitor (IPM) 2.6
- CiscoWorks Commons Services 3.0.3 with CiscoView 6.1.2

Company XYZ is considered a Large Enterprise and would implement severs with 300 to 1500 devices per server. CiscoWorks LAN Management Solution website lists the following as server and client workstation requirements:

Disk space (both Solaris and Windows):

- 10 GB or more free space for LMS applications and data

Solaris server requirements:

- Dual Sun UltraSPARC IIIi or dual Sun UltraSPARC IIICu for Ciscoworks LMS 2.5.1 Large Enterprise
- Memory: 4 GB
- Solaris 8 or 9

Windows server requirements:

- Dual 2.8 GHz Intel Pentium IV or Dual 2.8 GHz Intel Xeon processor for CiscoWorks LMS Large Enterprise
- Memory: 4 GB

- Windows 2000 Professional with Service Pack 4
- Windows 2000 Server with Service Pack 4
- Windows 2000 Advanced Server with Service Pack 4
- Windows 2003 Standard and Enterprise Edition with Service Pack 1

Client workstation requirements:

- Disk Space: Solaris 1 GB swap space
- Disk Space: Windows 1 GB virtual memory
- Memory: 512 MB
- IBM PC-compatible system with at least Intel Pentium IV processor
- Windows 2000 Professional with Service Pack 4
- Windows 2000 Server with Service Pack 4
- Windows 2000 Advanced Server with Service Pack 4
- Windows Server 2003 Standard and Enterprise Edition with Service Pack 1
- Windows XP with Service Pack 2
- Solaris 8 or 9

CiscoWorks Browser interface requirements:

- Internet Explorer 6.0 Service Pack 1 – Windows 2000, Windows Server 2003
- Internet Explorer 6.0.2900.2180 – Windows XP
- Netscape Navigator 7.1 and 7.2 – Windows 2000, Windows Server 2003
- Netscape Navigator 7.0 – Solaris 8, Solaris 9

- Mozilla 1.7 and 1.7.5 – Windows 2000, Windows Server 2003, Windows XP, Solaris 8, Solaris 9
- Java Plug-in version 1.4.2_08 (CiscoWorks Campus Manger and Internetwork Performance Monitor only)

CiscoWorks LMS consists of operationally focused tools capable of fault management, scalable topology views, sophisticated configuration, Layer 2 and 3 path analysis, voice-supported path trace, WAN performance troubleshooting, end-station tracking, and device troubleshooting (CiscoWorks LAN Management Solution 2.5.1, p.2).

CiscoWork Resource Manager Essentials is used to keep track of software versions, update devices when scheduled, and monitors the change log. CiscoWorks Server is used to integrate third-party applications and other Cisco management tools, such as IBM Tivoli and Cisco Information Center (CIC).

CiscoWorks utilizes security information maintained in Cisco Secure Access Control Server (ACS) to simplify management of user privileges. Cisco ACS allows for defining of user roles and secured user views of specific devices, group of devices or by geographic or logical network segments (CiscoWorks LAN Management Solution 2.5.1)

Chapter V: Discussion

Introduction

Company XYZ has a network of approximately 12,000 Cisco routers and switches. Other devices on the network are 3Com switches, Bay/Nortel routers and switches, Synoptics hubs, and F5 load distributors, as well as numerous firewalls and servers. There is a need to have a network configuration and change management solution in place to control and administer changes to these devices. Company XYZ uses the following tools for network management and administration:

- BMC Remedy Action Request System – Used for Incident Records, Change Management Records, and Problem Management Records.
- Cisco Information Center (CIC) – Used for alarm and event management in which Remedy Action Request Incident records are generated for trouble shooting and diagnosis.
- Peregrine Asset Center – Used for inventory control of devices and part numbers for Company XYZ locations.
- CiscoWorks LAN Management Solution 2.2 – Used for Cisco routers and switch IOS and configuration back ups. Also used to administer network changes at scheduled times, IOS upgrades, and global configuration changes such as passwords.

The tool used for changes, CiscoWorks LAN Management Solution 2.2 is at the end of life. According to Cisco's website for EOS/EOL for CiscoWorks LAN Management Solution 2.2, the following are important upcoming dates:

- July 31, 2006. End of Software Maintenance Release Date. This is the last date that Cisco Engineering may release any final software maintenance releases or bug fixes. After this date, Cisco Engineering will no longer develop, repair, maintain, or test the product software.
- July 31, 2006. End of New Service Attachment Date. This date is for equipment and software that is not covered by a service-and-support contract, this is the last date to order new service-and-support contract or add the equipment and/or software to an existing service-and-support contract.
- July 31, 2007. End of Service Contract Renewal Date. This date is the last date to extend or renew the service contract fro the product. The extension or renewal period can not extend beyond the last date of support.
- July 31, 2008. Last Date of Support. This is the last date to receive service and support for the product. After this date, all support service for the product are unavailable, and the product becomes obsolete.

Company XYZ does have a service-and-support contract with Cisco, so this does give them a year or so to implement an alternate solution or decide to upgrade to the current version of CiscoWorks.

Limitations

Limitations to this research project are as follows:

1. This research study is for Company XYZ. The researcher is limited to network configuration and change management issues affecting only Company XYZ.

2. This research does not explain how to install and support the software for network configuration and change management. This research will compare available options that will meet Company XYZ current and future needs.
3. This research does not test the software options. Due to the availability for vendors to provide demonstrations on Company XYZ's network infrastructure.
4. The NCCM vendors will need to be brought into Company XYZ to do their own evaluation of the company infrastructure. At that time, they will provide a detailed proposal to company XYZ, detailing unanswered questions. The researcher was limited for this initial product comparison with public knowledge which is available on the various NCCM vendors' websites.

Conclusions

Company XYZ is using CiscoWorks to successfully make and administer configuration changes with the assistance of human interaction. The current servers, Sun Microsystems Fire v250 running Solaris 5.8 operating systems may be some of the latency issues that users reported in the survey. Upgrading the servers to Windows 2000/2003 or Sun Solaris 8, 9, 10 may reduce time it takes to implement IOS changes, due to the current demand on the server's processor when there are multiple upgrades going on at one time. The good news for Company XYZ is their current Network Support staff are using new enough workstations, so there is only a need to address what platform and how many severs do they need to purchase.

The Netconfig and Distribute by Device job failures can be reduced by implementing change control process and guidelines to address the issue that jobs should not be run at the same time to the same device on the current system.

AlterPoint Device Authority, Emprisa E-NetAware, Opsware Network Automation System, and Voyence Control NG were identified as potential replacements since they are focused on larger enterprise networks. The vendors have a various selection of supported devices. Example of devices are routers, switches, firewalls, wireless access points, and load balancers. The list showing all supported devices is located in Appendix F: NCCM Supported Devices. Not all network change and configuration vendors support all devices, possibly a way of gaining competitive advantage by offering alternative choices. This may be true with third party integrations as listed in Appendix I: NCCM Integrations.

The network configuration and change management solutions address the key issues, automation, security, and audit and compliance control. These solutions have the following benefits:

- Change automation to reduce network downtime.
- The ability to revert to previous known valid configuration.
- Increase staff efficiency. Allowing staff complete other tasks versus manually making changes.
- Securing the network by administering Role Based Access Control.
- Notification when there is a change in network topologies. Identifies if the change is authorized or not.

- Compliance reports built into systems for various government and financial guidelines, for example, Sarbanes-Oxley and Gramm-Leach-Bliley Acts.

Server and end user workstation requirements are compared in Appendix D: NCCM Server Requirements. The servers are either Microsoft Windows 2000/2003/XP Professional or Sun Solaris 8, 9 or 10 operating system. Workstation requirements are compared in Appendix E: NCCM Workstation Requirements. End user workstations are either Microsoft Windows 2000/2003/XP Professional operating system. The processor is either an Intel Pentium III or IV with 256 MB or 512 MB memory. The end user interface is either Microsoft Internet Explorer, Netscape, Firefox or Mozilla.

Useful additions to a few of the solutions did stand out as unique and would assist in addressing network changes and isolation of issues relating to that change. Opsware Network Visualization is a tool used to create a network topology map to identify the Layer 2 and 3 interfaces of the devices that have changed. AlterPoint offers syntax verification checking before the change is being implemented. This is a nice feature to reduce the need for either manual intervention or reverting to previous configuration. Company XYZ has a number of Netconfig failures due to syntax errors with CiscoWorks LAN Management Solution 2.2.

CiscoWorks LAN Management Solution 2.5.1 is for managing only Cisco networks. There are change and configuration tools designed for Cisco IOS built into the application suite. The CiscoWorks suite does address security issues by using the Cisco Secure Access Control Server to administer role based access, as well as logical,

geographical and specific device access. There is the ability to pull various reports to meet compliance requirements.

Recommendations

Due to the proprietary and confidential information requested from the various network configuration and change management vendors; AlterPoint Device Authority, Emprisa E-NetAware, Opsware Network Automation System, Voyence Control NG, and an upgraded version of CiscoWorks 4.0; there needs to be a request by Company XYZ's management to have these vendors complete their own analysis of the network infrastructure. It is at this time that information such as pricing, support costs, licensing, training for network staff, number of devices per server, how devices will be imported into system, and other issues will be disclosed to Company XYZ. A list of questions for the vendors is located in Appendix B: Questions for Network Configuration and Change Management Vendors. These questions will need to be addressed at the time of the vendor's presentation and proposal to Company XYZ.

The vendors will complete their analysis of Company XYZ's infrastructure and present a proposal addressing what they feel are the needs to successfully implement their network configuration and change management solution. During this presentation, it is suggested that there are managers, as well as representatives from the various departments within Company XYZ Network Operations and Engineering Services staff, so that each departments concerns can be addressed and taken into consideration in selecting the replacement to CiscoWorks LAN Management Solution 2.2.

Benefits gained from selecting the right solution will be reducing network down time, improving network operations support staff efficiency, manage changes, security,

and compliance controls. These solutions will allow staff the opportunity to address other issues and not rely on time consuming tasks that an automation system can assist with. These benefits will in turn allow for greater network availability for Company XYZs' internal and external customers.

References

AlterPoint Solutions Areas: Change.(n.d.) AlterPoint Inc. Retrieved April 23, 2006 from http://www. AlterPoint.com/solutions/areas/change.html

AlterPoint Solutions Areas: Compliance.(n.d.) AlterPoint Inc. Retrieved April 23, 2006 from http://www. AlterPoint.com/solutions/areas/index.html

AlterPoint Solutions Areas: Security.(n.d.) AlterPoint Inc. Retrieved April 23, 2006 from http://www. AlterPoint.com/solutions/areas/security.html

Ciampa, Mark. (2005). *Security Guide To Network Security Fundamentals* (2nd ed.) Boston, MA: Thomson Course Technology.

Cisco Info Center. (n.d.) *Cisco Info Center Introduction.* Retrieved April 20, 2006 from http://www.cisco.com/en/US/products/sw/netmgtsw/ps996/index.html

CiscoWorks LAN Management Solution 2.2 Introduction. (n.d.). Retrieved April 17, 2006 from http://www.cisco.com/en/US/products/sw/cscowork/ps2425/products_data_sheet09186a00800a9e97.html

CiscoWorks LAN Management Solution 2.5.1.(n.d.). Retrieved April 22, 2006 from http://www.cisco.com/en/US/products/sw/cscowork/ps2425/products_data_sheet0900aecd803fd8eb.html

Colville, Ronni J. (March 13, 2006). *CMDB or Configuration Database: Know the Difference.* Gartner Research.

Dubie, Denise. (2004). *Network Configuration tools evolve*. Network World. Retrieved October 17, 2005, from http://www.networkworld.com/news/2004/0216specialfocus.html

Emprisa Networks. *Products: E-NetAware Device Support.* Retrieved April 21, 2006 from http://www.emprisanetworks.com/corporate/layout/set/print/content/view/full/145

Emprisa Networks. *Products: E-NetAware Platforms* (n.d). Retrieved April 21, 2006 from http://emprisanetworks.com/corporate/layout/set/print/content/view/full/146

Emprisa Networks. *Solutions: Compliance Auditing & Enforcement.* (n.d.) Retrieved April 23, 2006 from http://www.emprisanetworks.com/corporate/layout/set/print/content/view/full/319

Emprisa Networks. *Solutions: Configuration & Change Management* (n.d.) Retrieved April 23, 2006 from http://www.emprisanetworks.com/corporate/layout/set/print/content/view/full/317

Emprisa Networks. *Solutions: OS Image Management* (n.d.) Retrieved April 23, 2006 from http://www.emprisanetworks.com/corporate/layout/set/print/content/view/full/431

Emprisa Networks. *Solutions: Security* (n.d) Retrieved April 23, 2006 from http://www.emprisanetworks.com/corporate/layout/set/print/content/view/full/320

EOS/EOL Announcement For CiscoWorks LAN Management Solution 2.2 Retrieved March 5, 2006 from http://www.cisco.com/en/US/products/sw/cscowork/ps2425/prod_eol_notice0900aecd802136a2.html

Lammle, Todd. (2002) *CCNA Cisco Certified Network Associate Study Guide.* Third Edition. Alameda, CA: Sybex, Inc.

Newton, Harry. (2005). *Newton's Telecom Dictionary* (21st edition.) Gilroy, CA:CMP Books

Opsware Inc. *Compliance Management.* (2006). Retrieved April 6, 2006 from http://www.opsware.com/products/networkautomation/compliance

Opsware Inc. *Configuration Management.* (2006). Retrieved April 13, 2006 from http://www.opsware.com/products/networkautomation/cnfgmgmt/

Opsware Inc. *Network Visualization.* (2006). Retrieved April 13, 2006 from http://www.opsware.com/products/networkautomation/visual anal/

Opsware Inc. *The Opsware Network for NAS.* (2006). Retrieved April 13, 2006 from http://www.opsware.com/products/networkautomation/ton/

Out-of-the-box Product Integrations Support IT Management processes and best practices. (n.d.). Retrieved April 23, 2006 from http:// AlterPoint.com/products/integration/

Taylor, Steve and Metzler, Jim. (March 3, 2005). *Change Management, Human Error, and Network Outages.* Network World. Retrieved April 17, 2006 from http://www.networkworld.com/newsletters/frame/2005/0228wan2.html

Voyence Inc. *Voyence Control NG.* (2006). Retrieved May 6, 2006 from http://www.voyence.com/documents/VoyenceControl_NG-DS-2-7-06.pdf

Appendix A: CiscoWorks Survey

Questions for Company XYZ Employees
Network Configuration and Change Management -CiscoWorks Survey

Thanks in advance for participating in gathering information on the use of Cisco Works!

CiscoWorks is a Network Configuration and Change Management (NCCM) software tool that is used help manage a Cisco-based network. This survey will provide information on the current use of Company XYZ's NCCM tool.

Due to security reasons, the following will be followed.

- The company will be referred to as Company XYZ.
- Confidentiality. Names will not be used.
- No specific network devices will/are to be identified. (IP addresses/DNS names/Building names, etc.)

By returning this survey, you are giving informed consent as a participating volunteer in this study.

Note: Questions or concerns about this research should be addressed to Todd Martin, the researcher.

---

1. Do you use CiscoWorks? (Yes or No) _____

2. How often do you use CiscoWorks? (mark X next to selection that best describes you)

   ____ Daily

   ____ 2-4 times week

   ____ 2-4 times a month

   _____ 2-4 times a year

3. What do you use CiscoWorks? (place X by all that apply)

   ____ Information Only

   ____ Device Inventory

   ____ IOS Upgrades

   ____ Configuration Backup

   ____ Port activations

   ____ Interface configurations

   ____ Access List configurations

   ____ IPSec Configurations

   ____ NetConfig or Distribute by Device Job Approver

   ____ Other (please specify) _____

4. How long does it take you to create CiscoWorks configuration job?
   _____(minutes)

5. Has your CiscoWorks job failed? (Yes or No) _____

6. If your CiscoWorks job failed, please indicate issue/reason for failure.
   (Syntax issue, Cisco Works server issue, other, etc.) Type answer.

7. If you use CiscoWorks for IOS upgrades, how long does it take to complete?
   (Knowing that there are bandwidth differences for sites, please provide approx.
   minutes) _____minutes

8. If you use CiscoWorks to run any reports, what type of reports and what is the
   report used for?

9. Do you create CiscoWorks jobs to back out of changes? Or do you rely on manual back out procedures? (Type answer)

10. How long did it take you to create the back out job? _____ minutes

11. How long does it take on average to back out of change? _____ minutes

12. Would you like to use a software program that allows revert to previous configuration? (Yes or No)

13. Any additional comments/issues/limitations you would like to make about using CiscoWorks. Please add below.

THANK YOU FOR YOUR PARTICIPATION!!

Appendix B: Questions for Network Change and Configuration Vendors

Questions for Network Change and Configuration Vendors

The following questions will be answered either by the potential vendors "white papers", website, documentation, or e-mail/phone contact with the potential replacement NCCM software companies.

1. What are key features of you Network Change and Configuration Management solution?

2. What is the number of devices (routers/switches) that your network configuration management solution will support?

3. What is the cost of software license?

4. What is the cost of license/number of license(s) to support 12000 devices (routers/switches)?

5. What are your licensing requirements?

6. What are the server requirements for your NCCM solution (operating system, hardware, etc.)?

7. What are the end user/client requirements for your NCCM solution (operating system, hardware, etc.)?

8. What other network management systems is your product compatible with? (Peregrine, HP Openview, etc.)

9. Does your product import/export configuration data to/from any third party applications?

10. Does your company identify and/or provide drawing of major components of system?

11. Does your company provide training with new purchase of software?

12. Is your product developed to be in compliant to run reports for compliance controls such as SOX, HIPPA, etc.?

13. Does your product rely on any 3rd party applications, not included in your packaged product?

14. How does your product integrate security – Authentication, Authorization, and Accounting?

15. How is your product, initially implemented and maintained on the server and client side?

16. What devices are supported by your product?

17. Does your product provide device audits (standard vs. production configurations)?

18. What type of reports does your product run?

19. How does your product discover devices on the network?

20. How does your product maintain standard configurations?

21. How does your product maintain backup configurations?

22. Does your product automate recovery from configuration errors?

23. Does your product provide standard templates?

24. Does your product provide "groups" for global changes?

Appendix C: Network Configuration and Change Management Vendors

AlterPoint DeviceAuthority

Headquarters:
AlterPoint Inc.
300 West Sixth Street Suite 2200
Austin, TX 78701

URL: http://www. AlterPoint.com/
E-mail: info@ AlterPoint.com

CiscoWorks LAN Management Solution 2.5.1

Headquaters:
Cisco Systems
San Jose, California

URL: http://www.cisco.com

Emprisa E-NetAware

Headquarters:
10301 Democracy Lane, Suite 200
Fairfax, VA 22030

URL: http://www.emprisanetworks.com/
E-Mail: info@emprisanetworks.com

Opsware Network Automation System

Headquarters:
599 N. Mathilda Avenue
Sunnyvale, CA 94085

URL: http://www.opsware.com/
E-Mail: info@opsware.com

VoyenceControl NG

Headquarters:
1801 North Glenville Drive
Richardson, Texas 75081

URL: http://www.voyence.com/
E-Mail: info@voyence.com

Appendix D: NCCM Server Requirements

Server Requirements	AlterPoint Device Authority	Emprisa E-NetAware	Opsware NAS	VoyenceControl NG	CiscoWorks 2.5.1
	Operating System:	**Operating System:**	**Operating System:**	**Operating System:**	**Operating System:**
	Microsoft Windows 2000/2003	Microsoft Windows 2000/2003/XP Professional			Windows 2000 Professional with Service Pack 4 Windows 2000 Server with Service Pack 4 Windows 2000 Advanced Server with Service Pack 4 Windows Server 2003 Standard and Enterprise Editions with Service Pack 1
	Sun Solaris 9	Sun Solaris 8,9, or 10		Sun Solaris 9	Sun Solaris 8, 9
	Redhat Linux ES3/AS3/ES4/AS4	Linux		Red Hat Linux ES3/AS3	
	Database Server:	**Database Server:**	**Database Server:**	**Database Server:**	**Database Server:**
	MySQL v4.1.9 Oracle 9i & 10g Microsoft SQL 2000			Postgres SQL	
	Hardware:	**Hardware:**	**Hardware:**	**Hardware:**	**Hardware:**
	MicrosoftWindows/Redhat Linux	Microsoft/Redhat Linux		Linux	Microsoft Windows
	1 GHz Pentium IV	1 GHz Pentium III		Intel IV 2 Ghz	2.8 GHz Pentium IV
	1 GB Memory	1 GB Memory		2 GB Memory	2 GB Memory Enterprise 4 GB Large Enterpise
	10 GB disk	80 GB Hardrive		2 ATA/SATA 40 GB 7200 RPM drives	
	UltraSPARC III			V210 UltraSPARC 1 GHz	UltraSPARC III
	2 GB Memory			2 GB Memory	
	20 GB disk			UltraSCSI two 146 GB 7200 RPM drives	

Appendix E: NCCM Workstation Requirements

	AlterPoint Device Authority	Emprisa E-NetAware	Opsware NAS	VoyenceControl NG	CiscoWorks 2.5.1
WorkStation Requirements	**Operating System:**	**Operating System:**	**Operating System:**	**Operating System:**	**Operating System:**
	Microsoft Windows 2000/2003/XP Professional			Windows 2000/ XP	
	Hardware:	**Hardware:**	**Hardware:**	**Hardware:**	**Hardware:**
	Intel Pentium III 700 MHz or Greater			Intel Pentium III 600 MHz	
	512 MB Memory	256 MB memory (recommended)/128 MB (required)		256 MB memory	
	100 MB disk			Non-volatile Storage: 25 MB	
	User Interfaces:	**User Interfaces:**	**User Interfaces:**	**User Interfaces:**	**User Interfaces:**
	Display Resolution: 1024x768 or greater	Display Resolution: 800x600 Resolution			
	Microsoft Internet Explorer 6 SP1 or greater with 128-bit encryption	Microsoft Internet Explorer 6.x and above		Microsoft Internet Explorer 6.0	
		Firefox version 1.x and above	Firefox 1.0		
		Netscape version 7.1 and above		Netscape 6.0+	
		Mozilla version 1.4 and above			
	Desktop Client: Integrated Network Environment (INE)				

Appendix F: NCCM Supported Devices

	AlterPoint Device Authority	Emprisa E-NetAware	Opsware NAS	VoyenceControl NG	CiscoWorks 2.5.1
Supported Devices	3Com	3Com	3Com	3Com	
	Adtran		Adtran	Adtran	
				Air Space	
	Alcatel	Alcatel		Alcatel	
				Altean Systems	
	APC		APC		
			Aruba	Aruba	
	Allied Telesyn				
	Avaya				
			BelAir Networks		
			Blue Coat		
	Check Point	Check Point	Check Point	Check Point	
	Cisco Systems	Cisco Systems	Cisco Systems	Cisco Systems	Cisco Systems
			Cyclades		
	Dell				
	Enterasys Networks	Enterasys Networks	Enterasys		
	Extreme Networks	Extreme Networks	Extreme Networks		
	F5 Networks		F5 Networks	F5 Networks	
			Force 10	Force 10	
	Foundry Networks	Foundry Networks	Foundry Networks	Foundry Networks	
	HP	HP	HP	HP	
	Juniper Networks	Juniper Networks	Juniper Networks	Juniper Networks	
		Kentrox			
	Lucent Technologies			Luncent Technologies	
	Marconi	Marconi	Marconi	Marconi	
				McData	
	Milan Technology			Milan Technology	
	Motorola			Motorola	

Appendix F: NCCM Supported Devices Continued

	Alterpoint Device Authority	Emprisa E-Netaware	Opsware NAS	VoyenceControl NG	CiscoWorks 2.5.1
Supported Devices Continued			Net App	Net App	
			Netopia	Netopia	
	Netscreen		Netscreen	Netscreen	
			Network Appliance		
	Nokia	Nokia	Nokia	Nokia	
	Nortel Networks	Nortel Networks	Nortel Networks	Nortel Networks	
			Packeteer	Packeteer	
		Pedestel			
			Procket Networks		
	Proxim				
				Radware	
	River Stone Networks			River Stone Networks	
			Secure Computing		
				Siemens	
				Symbol	
	Tasman Networks			Tasman Networks	
			Terayon		
		Vanguard			

Appendix G: NCCM Audit and Compliance Controls

	Alterpoint Device Authority	Emprisa E-NetAware	Opsware NAS	VoyenceControl NG	CiscoWorks 2.5.1
Audit & Compliance	Sarbanes-Oxley Act (SOX)		Sarbanes-Oxley Act (SOX)	Sarbanes-Oxley Act (SOX)	
	CISP		CISP		
	FFIEC				
	FIPS Publication 199				
	NSA Security				
	Cobit Controtol Objectives				
	Health Insurance Portability and Accountability Act (HIPPA)		Health Insurance Portability and Accountability Act (HIPPA)	Health Insurance Portability and Accountability Act (HIPPA)	
	PCI				
	Statement on Auditing Standards (SAS 70)			Statement on Auditing Standards (SAS 70)	
	Gramm-Leach-Bliley Act (GLBA)			Gramm-Leach-Bliley Act (GLBA)	
	ISO 17799				
	ITIL		ITIL		
				Payment Card Industry Data Security Standard (PCI)	

Appendix H: NCCM Security Controls

	AlterPoint Device Authority	Emprisa E-NetAware	Opsware NAS	VoyenceControl NG	CiscoWorks 2.5.1
Security					
	Change Notifications	Change Notifications			
					Cisco Secure Access Control Server
	Encrypt Data Repository				
		Encrypted user and device passwords			
	Deploy security configurations	Deploy security configurations	Deploy security configurations	Deploy security configurations	Deploy security configurations
			Historical reports of vulnerabilities to network devices for past 13 years		
	RADIUS				RADIUS
	Role Based Security Access				Role Based Security Access - specific devices, logical and geographical devices
	Secure Application				
	Secure Computing Safeword				
	Secure Protocols to communicate with devcies (HTTPS, SSH, SCP)	Secure Protocols to communicate with devcies (HTTPS)			
	TACACS+				TACACS+

Appendix I: NCCM Integrations

	Alterpoint Device Authority	Emprisa E-Netaware	Opsware NAS	VoyenceControl NG	CiscoWorks 2.5.1
Integrations	BMC Remedy ARS	BMC Remedy ARS		BMC Remedy ARS	
				BMC Service Impact Manger	
	CA Unicenter NSM r11			CA Unicenter NSM r11	
	Cisco Secure ACS	Cisco Secure ACS			
		Cisco Information Center (CIC)			Cisco Information Center (CIC)
	Cisco RME	Cisco RME		Cisco RME	
	Configuresoft				
		Dartware InterMapper			
	EMC Smarts			EMC Smarts	
	HP Openview NNM	HP Openview NNM		HP Openview NNM	HP Openview NNM
	HP Openview Service Desk	HP Openview Service Desk			
	IBM Tivoli	IBM Tivoli			IBM Tivoli
		Ipswitch What's Up Professional			
	Micromuse			Micromuse	
	Opnet				
	Peregrine AssetCenter				
	Preventsys				
	Secure Computing				
	Secure Elements				
		Smarts InCharge			
		Solar Winds Orion			
	Windows Server System				