



Conquering the Operational Challenges of Network Change & Configuration Management through Automation

White Paper

V. Balasubramanian
ZOHO Corp.


Abstract

Modern enterprises depend on network availability for business continuity. In heterogeneous networks, administrators face numerous challenges in properly managing device configurations, carrying out changes, ensuring compliance to regulations, and in minimizing network downtime triggered by human errors. This white paper discusses the challenges in detail and examines the traditional, manual configuration management. The ways to tackle the challenges, the need for an automated NCCM solution to simplify the job of administrators, the vital ingredients that one should expect in an NCCM solution and the factors to ponder before zeroing-in on an NCCM solution, have been dealt with.



Contents

The Challenge.....	3
A Look at Traditional NCCM Practices.....	4
Limitations of the Traditional Approach.....	5
The Way Out.....	6
What to Look for in an NCCM Solution.....	7
Scope of NCCM for your Business Role.....	14
Conclusion.....	15



The Challenge

Networks form the backbone of the modern IT and other enterprises. The components of the backbone - the network infrastructure, are quite complex and varied with the presence of hundreds or even thousands of mission-critical edge devices such as switches, routers, firewalls and others from dozens of hardware vendors. Enterprises make huge investments on procuring network infrastructure and employ highly skilled professionals to manage and administer the network infrastructure. Typically, a few administrators manage a large infrastructure.

Managing the network is a challenging task as business continuity directly depends on network availability. Even a few minutes of network outage could have a rippling effect on the revenue stream as critical business services get affected. And as business needs grow, network complexity also grows up exponentially. The enterprise naturally puts the squeeze on the few network administrators mandating them with the responsibility of ensuring network availability. Not just network availability, but also ensuring security and reliability, optimizing performance, capacity and utilization of the network fall under the ambit of the administrators.

Business needs are in a constant state of flux and administrators are required to respond to the needs often by configuring the network devices, which is a sensitive and time-consuming task. It requires specialized knowledge, familiarity with all types of devices from different vendors, awareness on the impact of changes, precision and accuracy. Naturally, the highly skilled network administrators carry out the configuration changes.

Ironically, most of the configuration changes are repetitive, labor-intensive tasks - for instance, changing passwords and Access Control Lists. Yet, as even minor errors in configuration changes to the devices in production carry the risk of

Skilled network administrators spend a significant part of their time on configuring the devices.

They find it hard to concentrate on strategic network engineering and administration tasks.

causing network outage, the skilled network administrators spend a significant part of their time on configuring the devices. They find it hard to concentrate on strategic network engineering and administration tasks.

Besides, with increasing security threats to mission-critical network resources and serious legal consequences of information mismanagement, enterprises everywhere

are required not just to follow standard practices, internal security policies, stringent Government regulations and industrial guidelines, but also demonstrate that the policies are enforced and network devices remain compliant to the policies defined. Ensuring compliance has become a priority for network administrators nowadays. This drives them take extra care while changing configurations.

Administrators also have to continuously monitor the changes carried out to the devices, as any unauthorized change can wreak havoc to the network. Organization expects the network administrator and the IT department to deliver operational efficiency continuously and contribute for cost-effective network management.

It is evident that administrators face pressures from multiple angles; but, how do they normally manage configurations?

Let us have a look at some of the traditional network configuration management practices:

- While carrying out changes, most of the administrators document the proposed changes. They login to each device separately and carry out the change. In case, the configuration changes are not successful, they will turn the configuration to the previous working state by undoing the changes as recorded by them in the documentation.
- In big enterprises with a large number of devices, the administrators cannot follow the 'change documentation' process. Instead, they develop custom scripts to push configurations to multiple devices. With the enormous diversity of hardware vendors, the administrators develop numerous custom scripts to suit the syntax of each device type.
- Some others juggle with fragmented tools to do specific tasks in configuration management. They correlate the output from each tool manually.
- Still worse, some administrators follow the haphazard way of carrying out changes to live equipment without any management plan. When errors in configuration cause network outage, they end up wishing that they could move the configuration back to a proper working version. They manually troubleshoot the cause.



When errors in configuration cause network outage, administrators end up wishing that they could move the configuration back to a proper working version.



The Limitations of the Traditional Approach

The manual way of configuring the devices suffer various disadvantages and serious limitations. The following are prominent among the many:

- The highly skilled network administrators spend most part of their precious time on doing repetitive, time-consuming configuration tasks. They get little time to focus on strategic network administration plans and tasks. This amounts to wastage of resource, cost and time.
- There is no provision to apply configuration changes in bulk to many devices at one go. Administrators have to logon to devices separately or at best execute many custom scripts to get the work done, which would be time consuming.
- Even simple tasks like rotating passwords of devices, viewing access lists etc. could prove uphill.
- As the number of devices grows, administrators find it difficult to respond to the business priorities that require frequent configuration changes. Possibilities of committing errors become bright.
- A trivial error in a configuration could have devastating effect on network security giving room for malicious hackers. The traditional approach has no provision to check configurations before deployment from the standpoint of security.
- Administrators lose track of configuration changes. As a result, configuration management becomes a daunting task. In the face of a network outage, troubleshooting becomes laborious. The mean time to repair (MTTR) climbs significantly.

Issues at a Glance

- ❖ *Wastage of skilled resources in repetitive configuration tasks*
- ❖ *Administrators require lot of time to do configuration changes*
- ❖ *Troubleshooting in the face of outages becomes monumental*
- ❖ *No provision to monitor unauthorized changes, security and compliance*
- ❖ *Unable to keep track of configuration changes*
- ❖ *No centralized control*
- ❖ *Lack of accountability for actions*

- There is no way to control the access to device configurations based on user roles. No way to check/prevent unauthorized configuration changes either.
- The traditional practice has no scope to ensure accountability for user actions. When something goes wrong due to faulty configuration change or when a security breach occurs, it would not be possible to trace the actions to a particular individual in the absence of audit trails.
- There is no provision to monitor and ensure compliance to government regulations, industry best practices and standards.

The Way Out

Conquering the complex, multifaceted operational and technological challenges of network configuration management is getting simpler nowadays with the availability of Network Change and Configuration Management (NCCM) solutions.

The NCCM solutions are designed to automate the entire lifecycle of device configuration management. The process of changing configurations, managing changes, ensuring compliance and security are all automated and the NCCM solutions prove to be powerful at the hands of network administrators. They help save time and ensure network uptime.

It is pertinent to quote here an user advisory note by Gartner in one of its research reports:

“Replace manual processes with network device configuration management tools to monitor and control the change process, reducing risk and enabling compliance policies to be enforced. These tools provide an automated way of maintaining network configuration, offering an opportunity to lower cost, reduce human error and improve compliance with configuration policies.”

(Source: Gartner Inc., Hype Cycle for Networking and Communications, 2007, 26 July 2007)

By leveraging NCCM solutions, administrators can put in place both proactive and



“These tools provide an automated way of maintaining network configuration, offering an opportunity to lower cost, reduce human error and improve compliance with configuration policies”



reactive configuration management strategies. Proactively, administrators can reduce manual errors and prevent unauthorized changes; when something goes wrong, they can react to the contingency within minutes by getting to the root cause or by rolling-back to the previous working version.

What to look for in an NCCM Solution?

The strategic requirements to be expected in an NCCM solution can be classified into the following five broad categories:

1. Configuration Management
2. Change Management
3. Compliance Management
4. Audit & Reports
5. Automation & Tools

Configuration Management

All actions related to creating device inventory, retrieving configurations, viewing, editing and uploading them back to the device, maintaining historical versions of configurations, comparing configurations and establishing role-based access control can be classified under Configuration Management.

Multi-vendor Device Support

Networks nowadays are heterogeneous and hence the NCCM solution should be vendor-neutral, capable of supporting devices from various hardware vendors. At the least, the solution should support all device types from all popular vendors. Otherwise, administrators will not be able to achieve the desired level of automation.

The Triple 'C's of Configuration Management

Since device configurations are directly connected with the security of the network infrastructure, the scope of NCCM has been expanded with a third 'C' making it NCCCM – Network Change, Configuration and Compliance Management. A good NCCM solution should be capable of automating all of the triple 'Cs'.

Discovery Option for Device Addition

Device Configuration Management starts with the addition of your devices to the NCCM solution. Networks typically have hundreds, even thousands of devices. It would be a labor-intensive task to add each device manually. The solution should have provision for discovering the devices in the network and automatically add them, in addition to other device addition options.

Communication Protocols

The NCCM solution should support a wide-range of protocols to establish communication with the device and transfer configuration files. Government and Industry regulations mandate communication to take place over a secure channel. Hence, the NCCM solution should support SSH, SCP in addition to other protocols like SNMP, Telnet and TFTP.

Secure Storage

The device configurations are sensitive data and if a malicious user gets hold of device passwords, he can wreak havoc to the network. Hence, the solution should have provision for storing the configuration files in encrypted form in the data storage. The database should be guarded against intrusion.

Informative Inventory

The NCCM solution should provide an informative inventory of the devices being managed. It should provide various details such as serial numbers, interface details, chassis details, port configurations, IP Addresses and hardware properties of the devices. Such an inventory would prove to be a powerful tool at the hands of the administrators enabling them to gain visibility into the network devices.

Inventory should depict details such as serial numbers, interface details, chassis details, port configurations, IP Addresses and hardware properties of the devices

Configuration Operations & Schedules

The NCCM solution should provide simple, intuitive options in the GUI to carry out various configuration operations such as configuration retrieval, viewing, editing and uploading configurations back to the device. There should also be options to schedule the operations for automatic execution at a future point of time.

Configuration Versioning & Comparison

Configurations retrieved from devices should be stored with proper versions. Further changes should be versioned in incremental order. There should also be provision for comparing any two versions of same device or different devices. The comparison should be depicted side-by-side in the GUI showing the difference very clearly.

Baseline Configuration

The NCCM solution should have provision for labeling trusted configuration version of each device as 'Baseline' version to enable administrators to rollback configurations to the baseline version in the event of a network outage. Baseline version can be considered as the 'best working configuration version'.



Role-based Access Control

For security reasons, in multi-member work environment, access to devices and configurations should be controlled based on various functional roles. While administrators should be able to view all configurations, others should have restricted access as assigned by the administrator. The NCCM solution should have provision for this.

Approval Mechanism for Configuration Upload

Uploading configuration changes to devices is an important task and requires due care and in-depth knowledge of configuration syntax. Faulty configuration changes could leave security holes. Hence, the security policy of many enterprises require certain types of changes carried out by certain levels of users to be reserved for review and approval by top administrators prior to the deployment of the changes.

Change Management

The operations related to managing configuration changes – monitoring changes on real-time, preventing unauthorized changes, sending notifications on changes, restoration to trusted versions etc. fall under change management.

Real-time Change Monitoring

Unauthorized, faulty or malicious configuration changes could drastically affect business continuity and hence it is essential to have the ability to monitor configuration changes in real-time and make the latest configuration available in the central repository so that administrators will immediately know when their network operations are at risk.

Quick Restoration to Trusted Versions

Real-time awareness about configuration changes alone is not sufficient to prevent network outages. There must be provision to take quick corrective action to set configurations in order by rolling-back to baseline or a previously working version.

Change Management Policies & Notifications

The NCCM solution should offer robust change management policies to enable administrators define the action to be initiated when a configuration change is detected. The action could be anything – automatically rolling back changes, sending an email notification, SMS to mobile, triggering an alert to the network monitoring system etc.

Compliance Management

Government & Industry Regulations

Apart from ensuring secure storage, secure data transmission, granular access restrictions and comprehensive auditing, there must be provision for checking configurations for compliance to government/industry regulations (HIPAA, Sarbanes-Oxley, EPHI, GLBA, PCI Data Security Requirements etc.). Violations should immediately be reported as alerts to administrators.

Best Practices & Standards

The NCCM solution should have provision for checking configurations for compliance to a defined set of standards or best practices. For example, Cisco provides the 'Gold Standard', which explains the recommended security settings for Cisco devices. There should be provision for validating compliance to any such standards. The administrators should be able to define their own custom standards and

compliance policies.

Configuration Syntax Checking

During planned configuration changes, one of the best ways to minimize network outages due to manual errors is to check the syntax of the configuration changes for correctness before uploading them to the device. The changed strings should confirm to the automatic syntax validation by the NCCM solution.

Compliance Reporting

There should be provision for examining compliance at all levels - on demand, automatically at regular intervals and whenever a change happens. Violations should immediately be escalated to the security personnel. Besides, comprehensive compliance reports should be generated for submission to compliance auditors. IT Managers should periodically receive automated compliance reports. Detailed information on the devices that are compliant and the non-complaint should be generated. In addition, in the case of violation, remediation capabilities should be available.

Audit & Reports

User Activity Tracking

All actions performed by the users of the NCCM solution should be properly recorded as audit trails. Information on 'who' changed 'what' and 'when' should be easily decipherable. This will ensure accountability for actions in the organization. There should also be provision for sending reports on user-activity to IT Managers periodically.

Tamper-proof Audit Logs

Audit trails recorded by the application should not only be accurate, but also tamper-proof. Otherwise, malicious users would delete the records to conceal their actions. Audit trails will then be of no use to fix accountability issues. Even when the permission to purge the trails rests with a trusted administrator, alarms should be generated when audit trails are deleted.

Informative Reports

The information on the entire network configuration management process in your

enterprise should be presented in the form of comprehensive, informative reports. The status and summaries of different activities such as device configuration details, changes in configuration, network inventory, conflict between startup and running configuration, device audit details, user activity, policy compliance details etc should be provided in easy-to-understand formats, assisting the network administrators to make well-informed decisions on device configuration. A summary of important events should be presented as 'Executive Report' to the IT Managers periodically.

Automation & Tools

Automation

The NCCM solution should provide a high level of automation for all time-consuming and labor-intensive tasks. Quite often administrators wish to apply same set of changes to multiple devices – for example, applying a security patch. The NCCM solution should have provisions for configuration templates to carry out these tasks. Schedules, provision for bulk operations should all be there to simplify the job of administrators.

Firmware Upgrade

One of the tasks frequently done by network administrators is upgrading the firmware of devices. Uploading/downloading of IOS images is another important task. The NCCM solution should provide secure utilities to do these activities.

Command Execution Tools

The NCCM solution should provide utilities and tools to execute various commands on the devices and display the output. For example, to view the 'Access Lists' or VLANs of a device, administrators will have to just click a button in the GUI instead of manually connecting to the device in the command line interface.

Powerful Search

In enterprises having a large number of devices, there will be requirements to do a quick search for a particular device in the inventory. Sometimes, the configuration database needs to be searched for specific words, strings, phrases or a combination of these in device configuration files. The NCCM solution should have a powerful search mechanism to facilitate these.

Database Backup & Disaster Recovery

However robust the application may be, there should always be provision for a reliable disaster recovery mechanism. Live backup of data is the best setup to have. At the least, there should be support for periodic backup and secure storage of data. Tools should be provided to do recovery from backup data quickly after a disaster.

Integration with External Identity Stores, Authentication Mechanism

The NCCM solution should be capable of importing users/user groups as such from external identity stores such as Windows Active Directory or an LDAP directory. Also, it should be capable of using the authentication service provided by the external identity stores, disabling the local authentication provided by the solution. There should also be provision for leveraging third-party authentication like RADIUS, TACACS, AD, LDAP etc.

There should be provision for leveraging third party authentication like RADIUS, TACACS, AD, LDAP etc.

Access from Anywhere

The NCCM solution should preferably be web-based providing access for authorized users from anywhere. In geographically distributed environments, the need for this would be very high.

High Availability

Once an NCCM solution is deployed in production in an enterprise, IT administrators would be heavily dependant on the application availability for configuration operations. Continuous availability of the solution would be crucial. In Geographically distributed networks, the need becomes all the more crucial.

Simple to Install & Use

The solution should be very easy to install and use. It should just act as a tool at the hands of the administrators not demanding cumbersome installation procedure and usage.

Affordable Price

Though the NCCM solution will provide high value for the buck by enabling

administrators manage the expensive network infrastructure, the cost of the solution should not be too high to damage your pockets.

Scope of an NCCM solution for your organizational role

An indicative list explaining how an NCCM solution could aid your day-to-day work based on your organizational role, is provided below:

IT Manager

Reduce network outages occurring due to faulty configuration changes; ensure business continuity

- Ensure that configurations comply to a defined set of standard practices, polices & Government regulations
- Get informative reports on your network and take informed decisions
- Automate device configuration tasks to reduce operation costs

Network Administrator / Engineer

- Maintain versions of device configurations in a secure, centralized repository and manage them from a single interface
- Monitor configuration changes in real-time
- Automate time-consuming, repetitive configuration tasks
- Carry out configuration changes to a large number of devices with precision and ease

Network Security Professional

- Ensure that network devices remain perfectly secure
- Prevent unauthorized configuration changes
- Keep track of 'who', 'what' and 'when' of configuration changes
- Ensure that configurations comply to the security policies of the enterprise

Some users tell why they use an NCCM Solution ...

Neil C. Perry, IT Manager, Stoops Freightliner-Quality Trailer, Inc

"We deployed the NCCM solution (ManageEngine DeviceExpert) to roll out configuration changes to numerous network devices. It has helped us save a great deal of time. The automated approach allows us to sleep at night knowing that we always have the most up to date configurations of our devices. It's an absolute must for network administrators of enterprises of all sizes".

Larry Ware, Federal Signal Global Network Boffin

"The NCCM solution (DeviceExpert) has proven a very useful tool to help Federal Signal, Inc. manage equipment from multiple vendors across multiple geographic locations. It has allowed us to effectively manage remote device configurations and implement effective change control for network infrastructure"

Kevin Spies, Manager, Network Operations, Lightyear Network Solutions .

"Before deploying the NCCm solution (DeviceExpert), we used to manually download configurations and were struggling to keep track of changes. The NCCM solution changed all that by storing configurations in a central repository and making them accessible via a web GUI. We were able to respond faster to change requests from customers"

Conclusion

Lack of efficient and effective device configuration management affects the business continuity of enterprises. Manual configuration of devices eat away the time and efforts of the skilled administrators, who are struggling to keep track of configuration changes. Increasing security threats and government regulations force enterprises to comply to standard practices and policies.

Automated NCCM solutions enable network administrators to take total control of the entire life cycle of device configuration management. Changing configurations,

managing changes, ensuring compliance and security are all automated. These solutions improve efficiency, enhance productivity, help save time, cost and resources and minimize human errors and network downtime.

With a good NCCM solution in place, enterprises can make best use of their network infrastructure. They can achieve increased network uptime and reduced degradation and performance issues.

Introducing ManageEngine DeviceExpert

DeviceExpert is a trusted solution for network administrators to take total control of the entire life cycle of device configuration management. It is a web-based, multi vendor network configuration, change and compliance management (NCCCM) solution for switches, routers, firewalls and other network devices. It serves as a secure repository for device configuration, helps in continuous monitoring of changes, provides change notifications and reports, helps in easy and safe recovery to trusted configurations and in automating all configuration management tasks.

www.deviceexpert.com



ZOHO Corp. (formerly AdventNet Inc.)
4900 Hopyard Rd., Suite 310, Pleasanton, CA 94588, USA
Phone: +1-925-924-9500 **Fax:** +1-925-924-9600
Website: <http://www.deviceexpert.com>
For Queries: deviceexpert-support@manageengine.com