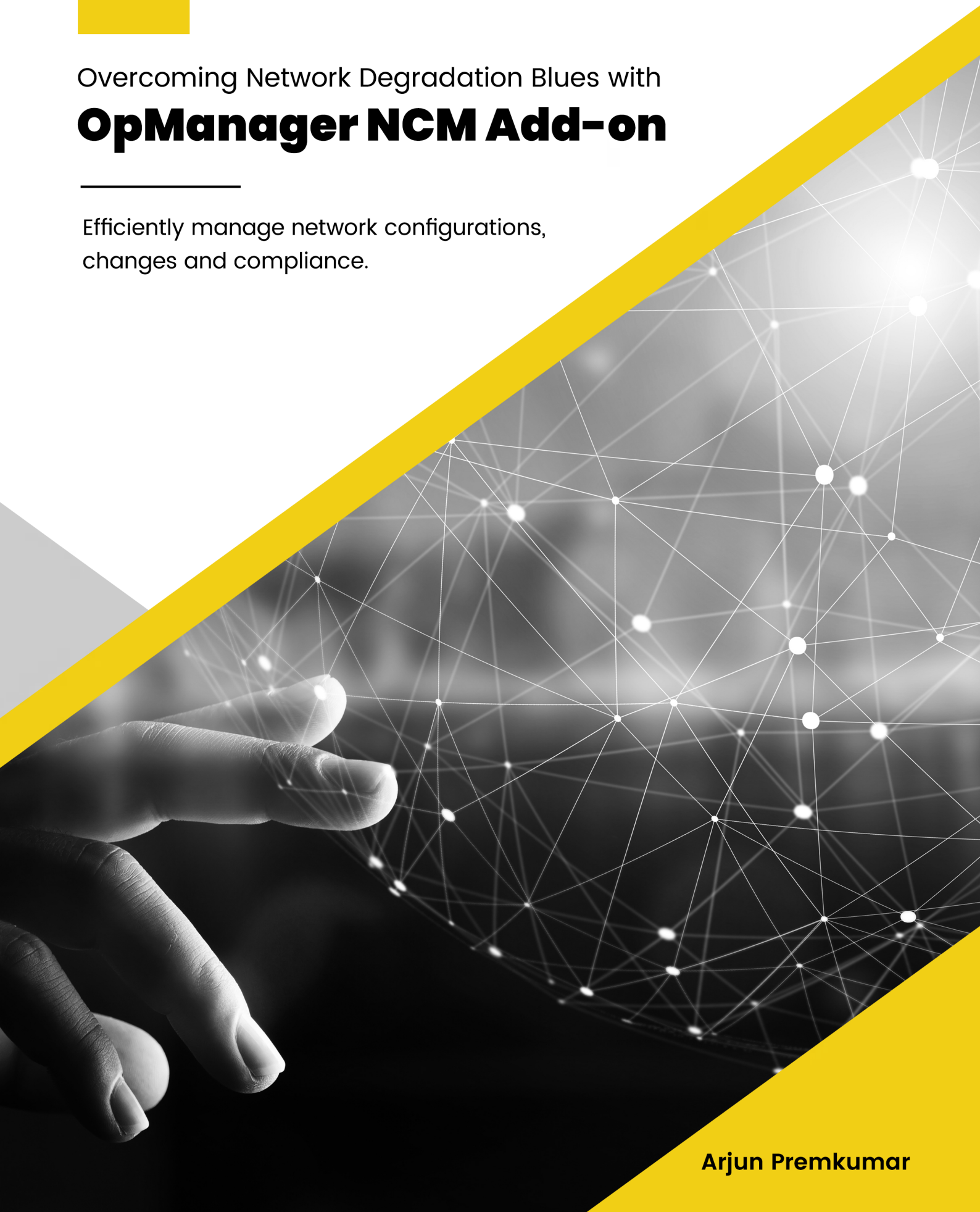
ManageEngine
Network Configuration Manager

Overcoming Network Degradation Blues with

OpManager NCM Add-on

Efficiently manage network configurations, changes and compliance.



Arjun Premkumar

Table of Contents

The Challenge

Enterprises – big and small, depend on network availability for business continuity. In heterogeneous networks with several devices across vendors, managing configurations becomes a daunting task for network admins. Even a few minutes of network outage could have a rippling effect on the revenue stream as critical business services get affected.

As business needs grow, modifications to the network infrastructure must also be made to cater to these needs. 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.

To keep the network up and running, it is essential to have a robust, reliable fault and performance management software that helps in effectively monitoring the network. With world-class ManageEngine OpManager in place, you have perfect control over the network monitoring arena. But, that alone may not be sufficient to prevent all network outages.

To keep the network up and running, it is essential to have a robust, reliable fault and performance management software that helps in effectively monitoring the network. With world-class ManageEngine OpManager in place, you have perfect control over the network monitoring arena. But, that alone may not be sufficient to prevent all network outages.

Network management experts repeatedly point out that more than half of the network outages and performance degradation issues are caused by faulty configuration changes. So, it is highly important to prevent network outages arising due to faulty configuration changes.

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. But, even the highly skilled are not immune to committing mistakes.

Ironically, most of the configuration changes are repetitive, labor intensive tasks - for instance, changing passwords and Access Control Lists (ACLs). With errors in configurations carrying the risk of causing a network disaster, the admins have to spend a significant amount of time 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 mis-management, enterprises everywhere are required to follow more than standard practices, internal security policies, stringent Government regulations and industrial guidelines. They are also required to 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 to 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 on the network.

Administrators also have to continuously monitor the changes carried out to the devices, as any unauthorized change can wreak havoc on the network.

Evidently, 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 enterprises with several devices, the administrators can't 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 use 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 have no way to restore the network with a proper working version of the configuration. They manually troubleshoot the cause.

The Limitations of the Traditional Approach

Manually configuring devices has various disadvantages and limitations. The following are prominent among the many:

- The highly skilled network administrators spend most parts of their precious time with repetitive, time consuming configuration tasks. They get little time to focus on strategic network administration plans and tasks. This amounts to wastage of resources, 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 difficult.
- 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 increase.

- 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.
- 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.
- There is no provision to generate reports of important network device hardware and configuration parameters.

The highly skilled network administrators spend most part of their precious time with repetitive, time-consuming configuration tasks. They get little time to focus on strategic network administration plans and tasks. This amounts to wastage of resources, cost and time.

Issues at a Glance

- Wastage of skilled resources in repetitive configuration tasks.
- Administrators require a lot of time to make 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.

The Solution

Conquering the complex, multifaceted operational and technological challenges of network configuration management requires the deployment of a Network Change and Configuration Management (NCCM) solution.

ManageEngine OpManager's NCM add-on comes into play here. OpManager NCM-add-on seamlessly integrates the Network Change and Configuration Management (NCCM) functionalities with the holistic fault and performance management capabilities of OpManager.

OpManager and NCM add-on together make Network Management not only efficient, but also truly centralized. From a single console, you will be able to monitor network performance, identify performance bottlenecks and manage device configurations. Having total control over device configurations will help you troubleshoot issues arising due to faulty configurations. In short, you will get end-to-end network visibility and also a handle to resolve conflicts.

What you can do with NCM add-on?

Manage configurations

- Manage devices across vendors with NCMs multi-vendor configuration support.
- Take regular backups and maintain versions of configurations to view, compare, edit, label and upload them from OpManager web GUI.

Take control of changes

- Monitor configuration changes in real-time, get notifications, prevent unauthorized changes and approve genuine changes.

Ensure compliance

- Define standard practices and policies and automatically check configurations for compliance.

Automate

- Automate repetitive, time-consuming configuration tasks like disabling TELNET service, changing SNMP community, forwarding syslog messages, changing the interface, changing passwords, updating NTP server entries, getting 'show version' output, uploading OS images / firmware upgrade, configuring banner message, deleting files from flash.

Audit

- Analyze the status of your network devices and configurations with intuitive reports. With reports on compliance, user activity, EOL/EOS, startup-running conflict and a lot more, simplify your auditing process.

Benefits of NCM add-on

The NCM add-on has been designed to automate the entire life cycle of device configuration management. The process of changing configurations, managing changes, ensuring compliance and security are all automated.

By leveraging the NCM add-on, administrators can automate the entire compliance monitoring process at all levels on demand, automatically at regular intervals and whenever a change happens. Regular checks can ensure your network's compliance with industry standards like Cisco IOS policy, PCI, HIPAA and SOX policies. Violations would immediately be escalated to the security personnel. Comprehensive compliance reports could also be generated for submission to compliance auditors. In addition, in the case of violations, remediation tips will also be offered. This will help enterprises in avoiding most of the network security issues.

NCM add-on will also help putting in place both proactive and 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 a trusted or stable version of the configuration.

- » End-to-end network visibility
- » Unified network management
- » Improved network uptime
- » Total control of configuration changes
- » Reduction in manual errors
- » Automation of routine configuration tasks
- » Compliance to industry standards

Automating Network Configuration Management will not only help networks remain compliant to the policies, but also make the network remain in top shape. Compliance to best practices will just become a way of life.

Conclusion

Lack of efficient and effective device configuration management affects the business continuity of enterprises. Manual configuration of devices is time-consuming for administrators, who are occupied with ensuring network uptime. Increasing security threats and government regulations force enterprises to comply to standard practices and policies.

OpManager NCM add-on infuses configuration management capabilities to OpManager's fault and performance management and brings in a complete network management solution. 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 OpManager NCM add-on in place, enterprises can make best use of their network infrastructure. They can achieve increased network uptime and reduced degradation and performance issues.

So, what are you waiting for? Download Network Configuration Manager with a 30-day free trial!

ManageEngine
Network Configuration Manager