BACKBOX

SOLUTION BRIEF

A New Roadmap for Network Configuration Management

Overview

Network Configuration and Change Management (NCM or NCCM) tools have been around for decades. During that time, these capabilities have become so integral to managing and protecting network and security infrastructure that NCM has evolved into a practice area: a collection of duties network engineers perform to take control of their network devices and proactively address issues before they escalate into major problems.

NCM best practices include:

- Backing up all configurations at least nightly, as well as before changes are made, so that rollbacks are enabled.
- Fine-tuning configurations to optimize them for the environment and then pushing them back out in bulk.
- Managing and executing OS upgrades to mitigate known vulnerabilities and to add new features.
- Conducting compliance assessments – detecting configuration changes and reporting the difference.

Unfortunately, many network teams are now realizing that their approach to NCM isn't keeping pace with the needs of their organization or evolving networking models. The pain is real and getting worse. According to Uptime Institute's 2023 Annual Outage Analysis, configuration management failure is the most common cause (45%) of major network-related outages, with human error and management failures contributing to a considerable number of outages. Additionally, digital infrastructure outages are becoming more expensive, with more than two-thirds of all outages costing more than $100,000.

So, what's the problem?

Disconnect #1

Legacy NCM products are typically intended to be used with an engineer at the keyboard. Your ability to scale is limited by how much work the engineer can get done from the console.

Additionally, NCM tools are often integrated with monitoring tools. However, monitoring as a way of managing your network is rapidly losing effectiveness because it is alert-driven and lacks the advantages and insights that observability platforms deliver. Network engineers are inundated with alerts that tell them, “This is misbehaving,” but there’s no “So what.” This makes it incredibly difficult to quickly determine which alerts to focus on and what actions to take to handle the daily volume of alerts.

That’s the first part of the problem.

Disconnect #2

The second part of the problem is the move to the cloud. In addition to managing the legacy network, virtual networks and public cloud networks must also be managed. This requirement simply doesn’t align with traditional NCM tools and approaches.

configuration management failure is the most common cause

45%

of major network-related outages.

- Uptime Institute, 2023

EVALUATING A PATH FORWARD

These two disconnects are forcing many network teams to reevaluate their path forward. Security concerns about their vendor, outgrowing their tool’s capabilities, or their tool being antiquated have been compounding. The complexity of NCM across an on-prem and cloud environment and integration with modern DevOps processes is the tipping point.

If you’re among the millions of people who make New Year’s resolutions, think of it as having a nagging pain in your knee for months that you’ve been living with. But now you’ve resolved to get back into running, so you’re training for a 5K race and need to get it fixed.

Bridging the Gap

Implicit in the need to move from monitoring to observability and insights across on-prem and cloud environments, is the need to move from traditional NCM to API-driven, NetDevOps-style NCM with built-in automation capabilities. The intent is to help network teams bridge the gap and manage their hybrid, multi-cloud environment as one ecosystem at scale.

This philosophical shift toward network automation to handle NCM tasks started several years ago and was not undertaken lightly. Early approaches involved significant financial investment and time. Organizations launched big projects and took months to implement complex, multi-product platforms and build a roadmap of automation workflows. However, the approach was overly complex and assumed a skill that network engineers generally don’t have – programming. A year later, having spent hundreds of thousands of dollars on services, many organizations achieved only a small fraction of their automation projects.

A NEW Approach

However, when you reverse the approach and start by automating the most mundane and aggravating but critical work you do with basic out-of-the-box automations, you can take the engineer away from the keyboard to focus on more impactful work and enable your configuration management practice to scale and ensure network cyber resilience. As your maturity with automation grows, you can go deeper with the platform to add more complex automations and functionality to solve the automation gaps you still want to address.

Common use cases include:

- API-driven configuration backups and rollbacks: Instead of only using your NCM tool to back up your configurations as scheduled, backups (and if necessary, restores) can be triggered via API and automated as part of a change workflow. For example, when a change is made to the network, a backup can be taken just before and then again after post-checks have completed. Should the post-checks fail, old configurations can be rolled back with everything audited for a post-change analysis instead of a backup.

- Compliance audits and remediations: Reviewing configurations to ensure they meet your standards can be overwhelming for network teams. Instead, schedule audits nightly and use automation templates that define your requirements. Ensure new devices are compliant during onboarding or post-discovery by automating the installation of a golden configuration. Avoid configuration drift with automated checks and remediation, or open tickets in an ITSM for manual investigation and remediation.

- **OS updates and vulnerability management:** Instead of relying on inventory spreadsheets and their accuracy, automatically maintain a real-time inventory of OS versions. Prioritize and automate updates based on vulnerability state, including information like Common Vulnerabilities and Exposures (CVEs), CVSS score, whether vulnerabilities are currently being exploited, and more. Automate OS updates to recommended versions, including bulk upgrades to devices from many different vendors, and track equipment end-of-life data for better device security.

- **Integration with ServiceNow:** Many companies use ServiceNow as their single point of truth about the state of IT assets. With BackBox, companies can initiate ServiceNow trouble tickets and enrich tickets with network-specific data that helps network engineers save time and minimize disruption. Additionally, the ServiceNow CMDB can be used as the discovery repository for all network devices known by BackBox.

Conclusion

An approach to NCM designed for today's complex networks enables you to optimize your NCM practice across your entire network infrastructure with actionable insights and automations you've put in place based on your workflows and requirements. Before you know it, that 5K run has turned into a 10 miler, and you're just getting started.

About BackBox

More than 500 enterprises worldwide trust BackBox as their preferred network cyber resilience platform. BackBox supports network devices from over 180 vendors, offering thousands of pre-built automations and a no-code way to create new ones. BackBox empowers teams with the confidence to automate critical network processes, maintain business continuity during disruptions, and recover swiftly. From backups and OS updates to configuration compliance and vulnerability management, BackBox ensures that automations deliver consistent, reliable outcomes.

To learn more, visit backbox.com