# Table of contents

The challenge ...................................................................................................................................... 2  
The heterogeneous landscape ............................................................................................................... 3  
Historical network automation alternatives .............................................................................................. 4  
Network Configuration and Change Management .................................................................................. 4  
Network automation defined ................................................................................................................. 5  
Selecting a network automation solution ................................................................................................. 6  
Benefits of good network automation ..................................................................................................... 7  
  Use automation to reduce operating costs ........................................................................................... 7  
  Increase network uptime and stability ................................................................................................. 7  
  Improve and enforce network security ................................................................................................. 8  
  Compliance validation and enforcement = consistently configured ......................................................... 8  
HP Network Automation software .......................................................................................................... 8  
Case study: State of Kansas, USA ........................................................................................................ 10  
  IT improvements: ............................................................................................................................ 10  
  Business benefits: ............................................................................................................................ 11
The challenge

As businesses struggle to cope with today’s economic situation, IT managers are facing a complex array of challenges. On the one hand, IT is increasingly being identified as an area of potential cost savings—so IT budgets are at best remaining flat, but more likely being cut. This trend necessitates IT managers to find opportunities to reduce both OPEX and CAPEX expenditures. At the same time, strong IT leaders know that simply cutting back IT expenditures and doing less is not the answer—in fact, it is a prescription for making things worse. Efficiency and cost-effectiveness are key goals—now more than ever—but achieving them will require some investments. IT initiatives that automate and manage network operations can be the key to address the goals of efficiency and cost-effectiveness.

The network, once only a component of the business, is now the fundamental backbone by which business is conducted. Most organizations cannot maintain productivity if their network is unstable. Even a short disruption in the network can represent substantial financial losses.

Projects that are implemented with an eye toward achieving cost savings, typically place an ever increasing demand on the network engineering staff. For example, the wave of cost savings through network and server virtualization may consume less hardware, rack space, power, and be more energy efficient, but this server virtualization is driving the need for additional connectivity and 10G ports at the network edge. This complexity increases the amount of time required to troubleshoot problems and lengthens the time to deploy these new services.

IT managers also have an increasing and ever-changing problem with network security. Vulnerable devices and configurations, rogue access points, viruses/worms, distributed denial-of-service (DDoS) attacks, and disgruntled employees—the list of threats is long and growing. Effective network security measures add an increased layer of complexity to the network infrastructure causing an increased chance of network problems. In fact, up to 80 percent of outages and security incidents are due to manual network misconfigurations. A simple mistake, such as the application of an incorrect filter on a router interface, could open a hole in the perimeter through which unauthorized users, potentially malicious, could access sensitive systems. Addressing these issues with manual techniques is costly and time consuming.

All of these forces contribute to network complexity and make cost-effective network management an elusive goal. The only way out is automation. The HP Network Lifecycle Management tools help achieve this automation.

HP Network Automation (HP NA) software tracks, regulates, and automates configuration and software changes across globally distributed, multi-vendor networks, helping IT managers prevent errors and deliver measurable cost savings through process-driven network automation.

HP Network Automation automates the complete operational lifecycle of network devices from provisioning to policy-based management, compliance, and security administration. When combined with HP Operations Orchestration and Network Node Manager software, it also extends workflow automation beyond traditional network change and configuration management and addresses the full network management lifecycle. By supporting an exhaustive set of network devices, it gives IT organizations comprehensive coverage.
Automation can only be achieved through maintaining a consistently configured network. In order to automate, the first thing IT has to do is standardize the network, especially the configurations and software versions operating on the network. The same thought and work should be applied to the network as it is to retail chains. This standardization provides the organization with a predictable operating network, which is required for automating changes across the entire network. Only with a predictable network can an organization reduce time in resolving network incidents or deploying new services. This consistently configured network will reduce costs associated with audits and meeting compliance standards whether they be IT best practices, company standards, or government regulations. This paper outlines what IT organizations should consider when preparing to automate their networks.

The heterogeneous landscape

All IT groups face the challenges of network uptime, security, and compliance. Other challenges faced by IT groups to achieve consistently configured and automated network are: the heterogeneous landscape, a multi-vendor mix of network devices, network management tools, and authentication systems. Today, very few organizations are completely dependent on a single vendor. From embracing industry-leading capabilities to improving price leverage, most IT organizations have a network model with at least two device vendors. Even organizations that have managed to stay with a single network vendor discover that with the current acquisition climate, their once 100 percent Cisco network is now a mix of HP Networking, Check Point, F5, and Cisco, post acquisition. Replacing the equipment at the acquired company would be tremendously expensive, thus the team must manage the heterogeneous network. And, it is not just multi-vendor devices a team inherits post acquisition; IT groups must fold in various vendor management tools as well.

From this perspective, organizations are increasingly dissatisfied with point solution vendors and their islands of disparate information. IT departments need an integrated ecosystem of network management solutions that will leverage the collective data to minimize time to identify and repair problems as well as deploy new services. This is considered “must have” functionality by IT departments and is one of the driving forces behind the need to adopt a Configuration Management Database (CMDB).
Historical network automation alternatives

IT organizations regularly employ fault management and ticketing systems to manage the network. These systems deliver the monitoring and change ticketing capabilities needed for network operations. These solutions do not, however, deliver any configuration management or automation capabilities. IT organizations have typically built their own scripts and utilities leveraging programming languages such as Expect or Perl. This increases the overall costs associated with developing, maintaining, and supporting these various scripts. Additionally, they typically don’t provide a centralized authentication and utilization model so they are not consistently used. Therefore, these in-house developed solutions have a dubious track record in reducing network management costs.

Over the last several years, more reliable and proven solutions have emerged and are referred to as Network Configuration and Change Management (NCCM) applications.

Network Configuration and Change Management

NCCM systems have existed since the mid 1990s, most recently gaining attention as multi-vendor NCCM tools emerged in 2000. The original goal of NCCM was disaster recovery, whereas the solution stores all device configurations and provides methods to recover from configuration problems. These tools have expanded in recent years to include asset management, batch script processing, compliance validation, and extensive reporting capabilities.

All IT organizations will benefit from the deployment of an NCCM system, regardless of the heterogeneous nature of the environment. A complete NCCM strategy provides a solid foundation upon which significant gains in network availability and automation can be achieved.

However, most NCCM tools fall short when you consider the challenges faced by today’s IT departments. NCCM systems only focus on the configuration management aspect of the network. There are critical areas specifically security, automation, and integration with server automation and fault-management applications that are not addressed. These areas have become increasingly important with the cost reductions, security, and compliance.

Automation capabilities within most NCCM systems are script based, a small step up from the homegrown scripts IT organizations have used for years. Furthermore, most NCCM tools lack the centralized control demanded by the security and compliance regulations today. With most NCCM tools, engineers and operators have the application or client installed on their local workstation, capable of connecting directly to the device and running scripts.

The entire platform relies on an ad-hoc approach of writing scripts and executing them on the fly. There is a lack of centralized control and management. For example, a user schedules a configuration change based on the existing configuration of the device. If, before the change is deployed, the configuration is altered in a break fix emergency operation, then the pending change, based on the original configuration, will cause network problems when deployed to the device. The NCCM system’s lack of control over this automation scenario jeopardizes network stability and undermines the promise of centralized consistency enforcement and auditing capabilities.
Despite their promise, NCCM systems do not deliver all the capabilities needed by today’s IT departments. Organizations need a solution that will provide:

- An engine to deploy error-free services with limited engineers
- A centralized model so that information can be obtained quickly and services can be delegated
- Configuration and asset management information in a relational data model
- Automated compliance validation and enforcement
- Extensive searching and reporting capabilities
- Built-in automation between configuration, fault, and performance management
- The ability to build automation across IT organizations, including network and server groups
- Ease of use, especially in early adoption and routine usage
- Robust logging and audit for traceability, accountability, and troubleshooting

**Network automation defined**

Automation is defined as the act of implementing the control of equipment with advanced technology; usually involving electronic hardware. Another definition simply states automation increases productivity. Given the current issues, a little automation within network operations could provide substantial productivity gains. Because of this, it seems that automation would be the next step in the evolution of NCCM tools. These NCCM applications should reduce the common repetitive, manual, and time consuming network activities.

Examples include deploying new services throughout the network, changing passwords, delegating simple changes to helpdesk staff, maintaining an up-to-date network configuration management database, and automatically checking compliance. By reducing the need for time-consuming manual actions, automation will enable companies to dramatically decrease their operating costs while improving the quality and consistency of the network. This would also result in decreased downtime and increased network stability. Automation would provide organizations with immediate visibility into every detail of their complex and changing networks as well as seamless automation of network maintenance and configuration activities. Since every company’s automation needs will be different the application must provide an open and flexible platform to integrate with existing applications. Automation extends beyond the basic capabilities of traditional NCCM systems to deliver complete automation of complex multi-vendor network operations.

Automation should enable organizations to maximize the value of their IT organization, freeing highly skilled engineers from manual tasks so they can focus on key business initiatives and deliver the quality of services the business demands. Functionally, network automation should deliver a holistic solution, including intelligent change monitoring, integrated change and fault management, compliance enforcement, vulnerability detection, software deployment, and inventory management. Network automation should be a fundamental component of all data center management strategies.

Powerful and scalable automation solutions often include a centralized model: A system that provides a self-service solution to current network data yet with granular authorization control to provide the correct level of access to information and tasks. Network security will be increased because employees can access real-time and accurate data without having to access the network devices directly. In fact, without a centralized model, a NCCM solution could do drastic damage to the network. A benefit of a centralized model is to provide the required checks and balances for a secure, compliant, and stable network without restricting department productivity.
Selecting a network automation solution

A network automation solution has, at its foundation, a solid configuration management (CM) system. A robust CM system can be defined as containing the following capabilities:

- Fast time to value
- An intuitive, easy-to-use user interface
- Requires minimal time and resources to deploy and manage
- Immediate value through intelligent device discovery and data population
- Real-time change detection and up-to-date database
- Easy-to-search detailed relational asset and configuration database
- Broad device coverage with regular updates and customer extensible
- Multi-variable, multi-device configuration, deployment, and provisioning
- Complex configuration, software and running-state validation, and enforcement
- Integration with network fault and performance management applications
- Inter-relationships between network switches and servers
- Granular role-based permission model
- Multi-tenancy support to partition device and content
- Geographically distributed architecture for scalability and high availability
- Automated reporting capabilities

Second, a network automation system must provide sophisticated automation capabilities. It is important that the system includes rich automation content out of the box, but it is more important that the system allows users to easily develop their own automation content. The system should inherently use automation within its own design. For example, if one transfer protocol or password fails, it should automatically try alternative ones. The solution must include well-documented application program interfaces and a command line interface so it can be automated and integrated with other management applications. The solution must also have the ability to trigger specific tasks based on events or results of other tasks. The system should monitor itself and take action based on the events. For example, a network automation solution can detect that it is running low on disk space or that its FTP server has failed and then alert the appropriate contact or open a trouble ticket.

Third, a network automation system must encapsulate the centralized model with capabilities that are easy to use and do not hinder productivity. At the very minimum, it should include:

- A workflow and approvals engine, capable of modeling complex processes
- Highly granular permissions model spanning device access and user actions
- Robust permissions management, including notification when user permissions change
- Centralized access point for all network devices
- Full keystroke logging for all user/device interaction
- Network lockdown capabilities
- Device automation conflict prevention
- Out-of-the-box integration with other control systems, such as, Lightweight Directory application protocol/Active Directory

Fourth, a network automation system must provide built-in sophisticated redundancy and failover capabilities. Because of the central-oriented nature of the system, redundancy and failover are critical to make sure that users do not bypass the system. It should provide geographically distributed architectures.
Fifth, a network automation system must provide highly-flexible and easy-to-use extensibility features. The system must offer out-of-the-box integration with all major management systems and an easy process to integrate with in-house developed systems. These highly-flexible extensibility capabilities include the ability to accept dynamic feeds of automation content/system commands, from a website or third-party system.

Sixth, the system must deliver an immediate return on investment.

With all of these requirements, the system must still be easy to install and configure, intuitive and straightforward to use. The solution should not lose the efficiencies gained through automation because it, in itself, requires a tremendous deal of maintenance or is cumbersome and difficult to use. The system should allow for a staged rollout, deploying the system on the network with limited capabilities, and then increasing the automation and control as the team becomes comfortable using it.

Seventh, the system must provide the ability to validate the configuration, software, and the running state of multi-vendor devices. A consistently-configured network consists of more than the device configuration. The system should provide the ability to create complex and powerful rules that reflect real-world scenarios. For example, a customer might need to make sure that two routers running a specific feature set is configured for Hot Standby Router Protocol and that they are operating correctly.

Benefits of good network automation

Automating the network is a proactive solution to address network management costs. For the network manager, it delivers the following benefits:

Use automation to reduce operating costs

Network automation provides a task engine to systematically execute changes across the entire network regardless of vendor. This reduces the time to deploy new network services, resolve identified problems or automate scheduled maintenance tasks. Another benefit is reducing the number of off-hours required by engineers to implement network changes. Organizations commonly report that their staff can design and test the planned changes. After they are comfortable with the saved changes they can schedule them to execute during change windows and alert them if they fail.

The network automation can automate multi-step and complex processes. For example, a task to upgrade the software on a device may involve several preliminary steps to determine if the software upgrade is appropriate for the device. Flexible extensibility of network automation solutions with event-triggered actions allows for integration and automation of any job, even jobs that span multiple management systems or IT department, for additional cost reductions and organizational efficiencies.

The automation engine should be capable of executing scripts written in any language to leverage existing automation capabilities already present in the environment.

The built-in device conflict resolution enables that the automation jobs are accurate and successful. Detailed error reports and analysis allow for swift identification and classification of failures for easy remediation.

Increase network uptime and stability

With real-time change detection, IT dramatically increases visibility into the network situation, precisely knowing who made changes, what changes were made, and when they happened. In addition, with the automation capabilities, any change can be rolled back to the previous, known good state, decreasing network downtime.

With out-of-the-box integration with other systems, users have better insight into network issues. For example, a configuration change is linked automatically to the specific fault incident and trouble ticket. Thus, the operator has a complete picture and the issue is faster and easier to resolve.
Network personnel are able to deploy network-wide configuration changes quickly, reliably, and systematically. They can easily and quickly repair configuration errors that are causing a network outage. Reports on network activity provide complete visibility of the IT environment with dynamic, out-of-the-box reports on operational activities. For example, a report could include the number of patches deployed in a week or who did what, when, and why.

**Improve and enforce network security**

Network managers and security personnel can implement strong user permissions over device access, such as by the time of day or on specific devices. Access privileges for users can be disabled quickly and reliably, without the need to reconfigure every device on the network. Because of the centralized model, devices can be configured to accept incoming connections from only authorized network automation systems, thus decreasing the risk of being hacked by a malicious user. In addition, network managers gain accountability for their teams’ activities with keystroke logs of actions and identification of who made each change.

The powerful automation capabilities within the network automation solution enable quick response to emerging network problems or threats. For example, the centralized device software management allows easy deployment and monitoring of device software, including identifying those OS versions that contain known vulnerabilities.

Real-time enforcement of best practice configuration standards ensures network standards are compliant at all times. With network automation, users can be prevented from deploying a configuration change that will violate the defined standards.

In addition, with the advanced network change control workflow and approvals enforcement, mistakes are prevented, contributing to the overall security, consistency, and stability of the network. If any security holes do occur, the flexible notifications immediately alert the appropriate staff.

**Compliance validation and enforcement = consistently configured**

Real-time enforcement of standard configurations and device operation enable consistent and securely configured network 24x7. With network automation, not just the configuration settings are enforced, but also the device operation and the associated change processes. Network automation facilitate compliance with policies and best practices by automatically validating proposed changes and providing an option to rollback unauthorized or non-compliant changes. The granular user permissions makes sure that only authorized personnel access devices or are allowed to automate changes on devices.

Out-of-the-box integration provides coordination with existing change control processes to make sure that the system easily maps into the existing ecosystem. As a result, IT personnel do not have to change their workflow, making the system easier to adopt. Workflow and approvals enables a smooth implementation of Information Technology Infrastructure Library (ITIL) or other disciplines to achieve IT compliance.

**HP Network Automation software**

The HP Network Automation software is a comprehensive solution that enables network automation to heterogeneous networks.

HP NA automates the complete operational lifecycle of network devices from provisioning to policy-based change management, compliance, and security administration. HP NA is a multi-vendor solution and supports thousands of different network devices from 70+ vendors.
HP Network Automation delivers the following capabilities:

**Network lifecycle management**—Takes a holistic approach to managing the network lifecycle, HP NA combined with HP NNM and HP Operations Orchestration software delivers a complete management and automation solution, which spans traditional IT silos. This approach provides unparalleled potential to enhance the overall impact of automating your network operations.

**Fast time to value**—Easy to install, deploy, and use. Customers experience immediate value through the automated device discovery and policy-based configuration. It is designed with a simple and intuitive Web browser designed specifically for network engineers and managers.

**Automation engine**—Creates complex automation flows, integrating internal and third-party systems. Leverage more than 200 system triggers to drive automation.

**Real-time change detection**—Improves network availability and change control by automatically detecting, tracking, and sending notifications for all device configuration changes. It also uses this information to maintain the accurate network CMDB.

**Policy-based change management**—Enables compliance with configuration standards, policies, and best practices by automatically validating proposed changes, deployment, and rolling back unauthorized or non-compliant changes.

**Policy-based and ad-hoc rollback**—Improves network stability and security by rolling back to a previous configuration either automatically or through user intervention.

**Workflow and approvals**—Automates multi-step complex processes and enforces change management best practices. Allows organizations to comply with ITIL best practices.

**ACL management and network lockdown**—Improves network device security by restricting device access and locking down ACLs.

**Network Node Manager i-Series 8.01/8.11 (NNMi)**—Rich out-of-the-box cross launch, data sharing, and task co-ordination with Fault Management, which is a key part of full network lifecycle management. Other integrations include EMC Smarts and Remedy.

**Process-powered network automation**—Integrates IT workflow and run-book automation to gain efficiencies and lower costs for IT process that cross multiple groups within the IT organization.

**Integration with HP BSA, BSM, and IT Service Management applications**—Enables faster troubleshooting and overall data center automation by providing device change history, location, and connectivity information to existing HP applications such as HP OpenView NNMi, Service Manager, Server Automation, and Operations Orchestration.

**Device run-time state policy compliance**—Automates checking compliance on an “as running” basis.

**Deploy software updates**—Ensures network devices are running the latest secure firmware or OS and eases deployment of new images to many devices simultaneously.

**Integrated software image download from Cisco CCO**—Facilitates faster, easier downloads of Cisco device images from Cisco CCO directly into HP Network Automation.

**Automated software synchronization and image management**—Creates a repository and synchronizes all device software images across your enterprise network. Use image management to automatically identify, download, and install the recommended software image for your network devices.

**Report on assets, operational activity, and regulatory compliance**—Reporting provides complete visibility of the IT environment with dynamic, out-of-the-box reports on asset information (for example, hardware, software, and configurations), operations activities (for example, number of patches and who did what), and regulatory compliance [for example, Sarbanes-Oxley Act (SOX), Health Insurance Portability and Accountability Act (HIPAA), and Gramm-Leach-Bliley Act (GLBA)].
Support for IPv6 and SNMPv3—Support for next-generation network technologies that allow you to support current and future protocol needs.

Diagramming and visualization, including layer 2 and 3 modeling—Generate a graphical representation of your network. Identify which devices are inactive or out of compliance. Use filters to immediately view isolated specific network segments. Capture a snapshot of the current state of the network, including topology and virtual LAN information. Identify the hosts connected to specific switches or interfaces by MAC address.

Horizontal Scalability architecture—Provides the ability to increase task throughput and reduce task deployment time by deploying multiple application servers.

Cisco IOS XR Support—The only vendor other than Cisco to support Cisco IOS XR-based devices

Bare Metal Provisioning—Rapidly deploy new network devices throughout the data center and networks using standard templates

Multi-Tenancy Support—Segment content, including policies, scripts, diagnostics, and password to individual customers or organizations

VoIP Support—First Network Configuration Management application to provide support for Cisco VoIP platform, including Cisco Call Manager.

Case study: State of Kansas, USA

Finally, we will review a real-life case study of a network lifecycle management deployment at the State of Kansas. As with many US state governments, Kansas relies on a heterogeneous infrastructure that spans dozens of agencies and services, including the departments of labor, corrections, transportation, revenue, the state’s Veteran’s Administration, Secretary of State, Social Services, and the Motor Vehicle Department. Some 22,000 employees, plus several hundred contractors, use the state’s IT infrastructure, as well as several thousand citizens who access services daily through agency websites.

The networking group of the state’s Division of Information Systems and Communications (DISC) department is responsible for a core network, connecting Topeka and Kansas City, and, to varying degrees, the infrastructure connecting the state’s 500 regional offices to that backbone. Altogether, it adds up to about 1,100 network devices—750 routers and 350 switches—serving 105 counties across 82,000 square miles.

The State of Kansas has been an HP customer since the early 1990s. They use a combination of HP network automation and management software tools. The results they have realized using these tools have been impressive. In just a matter of months, the group has been able to reduce the number of network management applications they need to maintain, and they’ve enabled their system administrators to work more efficiently. They have also laid the foundation for delivering long-term cost savings to the DISC organization and the State of Kansas.

More specific improvements include:

IT improvements:

- Replaced multiple tools with one, reducing management complexity
- Improved mean-time-to-repair by 15-20 percent
- Reduced incidents during major network events by 25-30 percent due to automated event correlation and root cause analysis
- Doubled the tier-one incident resolution rate

Saved more than 3,300 man hours per year using automated and integrated solution
Business benefits:

- Improved network availability
- Reduced operational costs by tens of thousands of dollars
- Reduced administrator training costs
- Empowered IT staff to be more proactive about service improvements
- Reduced business risk through IT standardization and automated control
- Achieved payback on investment in six months

DISC’s next goal is using the HP Network Automation software to further optimize his group’s ability to track and regulate network configuration and software changes. They’ll automate tasks like provisioning and integrate HP NA with HP NNMi to give them a single interface for fault and configuration management, making it easier to correlate changes with faults.

And because the state’s network administrators spend less time chasing and analyzing alerts, they have more time to devote to proactive management processes—which, in turn, helps improve the services the state can deliver across multiple departments and to citizens in all parts of the state.

To track, regulate, and automate configuration and software changes across globally distributed, multi-vendor networks with HP Network Automation software, visit: [www.hp.com/go/nasware](http://www.hp.com/go/nasware)