

Network Automation:  
A fundamental shift  
in network management

## The complex network

IT managers face many complex challenges today. The network, once only a component of the business, is now the fundamental backbone by which business is conducted. Few organizations can maintain maximum productivity if their network is unstable for long periods of time. Even a short disruption in the network can represent substantial losses. A recent Enterprise Management Associates (EMA) study found that downtime costs a company an average \$1,400 per minute. For a network with exceptional 99.9% availability, this still translates to over \$700,000 annually. With such serious financial consequences, Network Managers face intense pressure to eliminate all occurrences of network instability.

In addition to the demand for 100% network reliability, IT managers have a increasing and ever-changing problem in 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 a network problem. In fact, studies show that 80% 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.

Rapidly increasing in importance on the network managers list of challenges is regulatory compliance. From Sarbanes-Oxley to CISP, the accurate demonstration and enforcement of best practices and/or compliance standards is prohibitively expensive and difficult to do manually. Analysts estimate that compliance requirements are five times more costly to meet when done manually. Couple this with the fact that studies suggest that over 50% of the deficiencies reported by auditors are IT related and the management issues are clear.

While IT faces the challenges with keeping the network running, secure and compliant, the business continues to demand additional services to further increase operating efficiencies and company competitiveness. Organizations seek efficiency savings through IP telephony and productivity gains through remote access improvements, MPLS VPNs and WLANs. These new IT services increase the complexity of the network infrastructure and increase demand for even greater network availability.

All of these forces contribute to the overall network complexity and make cost-effective network management an elusive goal.

## The heterogeneous landscape

Of course, all large IT groups face the challenges of network uptime, security and compliance. For many organizations, however, there is an additional wrinkle that presents its own pitfalls; 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 best of breed capabilities to improving price leverage, most IT organizations have moved to 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% Cisco network is now a mix of Nortel, 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, its 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 data. IT departments demand an integrated ecosystem of network management solutions that will leverage each other and all of the collective data to maximize speed to identify and repair problems as well as deploy new services. This is considered “must have” functionality by innovative IT departments and is one of the driving forces behind the current trend to adopt a Configuration Management Database (CMDB).

Finally, in most organizations, necessary cost savings are being obtained from multiple departments, including IT. This forces the CIO to face certain realities:

- IT needs to increase network availability to support company productivity and critical applications
- IT needs to proactively deliver and maintain impenetrable network security
- IT needs to proactively enforce and validate compliance with government / internal regulations
- IT needs to adopt new technologies to remain competitive
- IT needs to provide all of the above with the same or fewer resources

To address these complex, multifaceted challenges, a new type of network management solution has emerged. Enterprises, governments, and service providers are turning to Network Automation to keep network management costs contained while providing the quality and responsiveness their organizations demand.

## Historical Network Automation alternatives

Large IT organizations regularly employ fault management and ticketing systems to manage the network. These systems deliver the monitoring and change management capabilities needed for project management and fault monitoring. These solutions do not, however, deliver any configuration management or automation capabilities.

More recently, two types of solutions have emerged for configuration management and automation: the Network Configuration and Change Management (NCCM) system and the Modeled Device Provisioning (MDP) system.

### **Network configuration and change management (NCCM)**

NCCM systems have existed since the mid 1990's, most recently gaining attention as multi-vendor NCCM tools emerged in 2000. The original goal of NCCM was disaster recovery, to store all device configurations and provide 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 can be achieved.

NCCM tools, however, 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, access control and hands free automation that are not even addressed. These areas have become increasingly important in this day of security, compliance and cost management. Automation capabilities within NCCM systems are script based, a small step up from the home grown scripts IT organizations have used for years. Further, they 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 no automation control. 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 pushed to the device. The NCCM system's lack of control over this automation scenario jeopardizes network stability and undermines the promise of increased uptime.

## Modeled device provisioning (MDP)

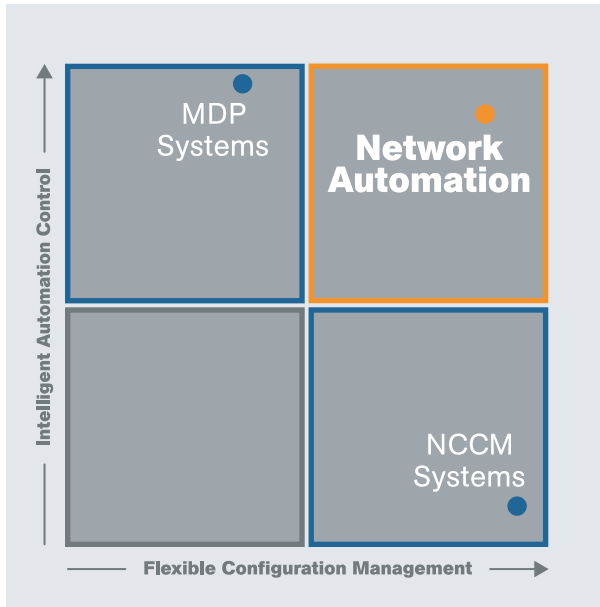
Modeled Device Provisioning (MDP) systems have existed since the early to mid 1990's. The most widely recognized example of an MDP system is the vendor-specific management tools, such as Nortel's Device Manager or CiscoWorks DeviceView. The goal of MDP systems is to remove the need to work directly with the device CLI and thus, remove some of the complexity of working with network devices. More recent examples of MDP systems, like NCCM systems, have been multi-vendor tools that attempt to obfuscate the entire device interface, regardless of vendor, into one, uniform GUI.

MDP systems provide benefits through the reduction in the number of specific device interface experts and the decrease in the number of configuration errors. MDP systems can make it relatively fast and error-free to roll out new services with limited network engineers. In addition, because the entire team uses the tool to make changes, organizations immediately inherit centralized control over the network, critical for increased security and regulatory compliance.

While the MDP vision is very compelling, MDP tools have not been able to deliver the panacea of error-free, low cost device provisioning they promise. The largest challenge is the limited device support MDP systems offer. Because the entire device UI must be abstracted, it is a long and sensitive process, susceptible to bugs from minor changes in OS versions. Often, companies can get, at most, 2 to 3 different vendors supported, and of those, limited model support. There is a long adoption time as the entire team must learn the new UI and methods to work with devices. Further, organizations cannot roll out the system in phases, to ease the migration towards centralized management.

Despite their promise, NCCM and MDP systems do not deliver the capabilities needed by today's large IT departments. Organizations need a solution that will provide:

- An engine to deploy error free services with limited engineers
- A centralized control model
- Configurations and asset management, including disaster recovery
- Automated compliance validation and enforcement
- Extensive reporting capabilities
- Ease of use, especially in early adoption and routine usage
- A phased rollout and/or adoption strategy



What is needed is a blend of the strengths of NCCM tools and MDP tools. Network Automation has emerged to deliver this sophisticated mesh of capabilities.

## Network Automation defined

Network Automation is the next step in the evolution of NCCM and MDP tools. Network Automation is an intelligent, context-aware software solution that removes the manual human element from network activities – completely automating manual processes, manual configuration activities and manual policy enforcement. Currently, 45% of network engineers spend their time on manual network activities. By eliminating the need for time-consuming manual actions, Network Automation enables companies to dramatically decrease their IT operating costs while improving the quality of the network, thus resulting in decreased downtime and increased network stability. Network Automation provides organizations with immediate visibility into every detail of their complex, changing IP networks as well as seamless automation of all network maintenance and configuration activities. Network Automation goes beyond traditional NCCM systems to deliver complete automation of compliance survey, management and enforcement, operations workflow and network lockdown of complex multi-vendor IT networks.

Network Automation enables 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 services the business demands. Functionally, Network Automation delivers a holistic solution including intelligent change monitoring & management, compliance monitoring & enforcement, security monitoring & network lockdown, vulnerability detection, patch management, inventory management with network discovery and disaster recovery. Network Automation is a fundamental component of all data center management strategies.

At the heart of Network Automation is the Centralized Control Model: a system that enforces strict access control and channels all network management activity through tightly controlled processes. Without the Centralized Control Model, Network Automation systems are simply NCCM tools that offer sophisticated automation capabilities. In fact, without the Centralized Control Model, a Network Automation system could do drastic damage to the network. The goal of the Centralized Control Model is to provide the required checks and balances for a secure, compliant, stable network without stanching 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:

- real-time configuration archival and restoration
- asset management
- batch script processing
- compliance validation and enforcement
- reporting capabilities

Second, a Network Automation system must provide sophisticated automation capabilities. It is important that the system include rich automation content out of the box, but it is equally important that the system allow users to easily develop their own automation content. The solution must also have mature automation capabilities including the ability to dynamically manage the results of automation jobs, automate task flow, self-manage required system resources / connections and automate system actions and behavior. For example, a Network Automation solution can detect that it is running low on disk space or that its FTP server failed to restart properly, and then alert the appropriate party or open a trouble ticket.

Third, a Network Automation system must encapsulate the Centralized Control Model with capabilities that are easy to use and do not hinder productivity. At the very minimum, it should include:

- A workflow & approvals engine, capable of modeling complex processes
- Highly granular permissions model spanning the two silos: 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 AAA, LDAP/Active Directory or Change Management systems

Fourth, a Network Automation system must provide sophisticated redundancy and failover capabilities. Because of the control-oriented nature of the system, redundancy and failover are critical to ensure users do not have to bypass the system.

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 home grown systems. These highly flexible extensibility capabilities include the ability to accept dynamic feeds of automation content / system commands, from a website or 3rd 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 straight forward 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. In other words, deploying the system on the network with limited capabilities, and then increasing the automation and control as the team becomes comfortable using it.

## Weighing the benefits of Network Automation

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

### **Increase network uptime and stability**

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

With the out-of-the-box integration with other network systems, users have better insight into network issues. For example, a configuration change is linked automatically to the specific 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 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, 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, including by time of day or by specific device. Access privileges for users can be disabled quickly and reliably, without the need to reconfigure every device on the network. Because of the Centralized Control 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 manager gain accountability for their team's activity with a keystroke log of actions on each device.

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

Real-time enforcement of best practice configuration standards ensures strict network security standards are obeyed at all times. With Network Automation, users are often automatically prevented from pushing out a configuration change that will violate the defined security standards.

In addition, with the advanced network change control workflow and approvals enforcement, mistakes are stopped before they happen, contributing to the overall security and stability of the network. If any security holes do occur, the flexible, powerful notifications immediately alert appropriate parties.

## **Compliance validation and enforcement**

Real-time enforcement of best practice configuration standards enforces compliance 24 x 7. With Network Automation, not just the configuration settings are enforced, but the actual change and workflow processes IT uses to manage the network. Network Automation ensures compliance with policies and best practices by automatically validating proposed changes, deployments, and automatically rolling back unauthorized or non-compliant changes. The granular user permissions ensures that only authorized personnel access devices or are allowed to automate changes on devices.

Out-of-the-box integration with helpdesk systems provides connection with existing change control processes to ensure that the Network Automation system easily maps into the management ecosystem. As a result, IT personnel do not have to change their workflow making the system easier to adopt.

Network control workflow and approvals enables smooth implementation of ITIL or other disciplines to achieve compliance.

## **Greater automation and lower total cost of ownership**

Network Automation provides the engine to automate multi-step, 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. The flexible extensibility with event-triggered actions allows for integration and automation of any job, even jobs that span multiple management systems, for lower total cost of ownership.

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

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

## Introducing the Opsware Network Automation System

The Opsware Network Automation System (NAS) is a comprehensive solution that enables Network Automation to large, complex, heterogeneous networks. Opsware NAS is the winner of 8 industry awards, including InfoWorld's 2005 Technology Product of the Year and Network World's Best of Tests 2005.

Opsware NAS automates the complete operational lifecycle of network devices from provisioning to policy-based change management, compliance, and security administration. Opsware NAS is a multi-vendor solution and supports over 400 network devices from 20+ different vendors.

The Opsware Network Automation System delivers the following capabilities:

**Real-time change detection** - Improves network availability and change control by automatically detecting, tracking and sending notifications for any configuration changes on a device.

**Policy-based change management** - Ensures compliance with 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 via user intervention.

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

**ACL management and network lock-down** - Improves network device security by restricting device access and locking down access control lists (ACLs).

**Integration with existing IT Systems** - Enables faster troubleshooting by providing device change history, location, and connectivity information to existing IT tools such as HP OpenView, Micromuse NetCool, BMC Remedy, EMC Smarts, and CA Unicenter.

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

**Report on assets, operational activity, and regulatory compliance** - Award winning reporting provides complete visibility of the IT environment with dynamic, out-of-the-box reports on asset information (e.g., hardware, software, configurations), operations activities (e.g., number of patches and who did what) and regulatory compliance (e.g., SOX, HIPAA, GLBA).

**For More Information**

If you would like additional information about the Opsware Network Automation System or Opsware Inc., please visit our Web site at [www.opsware.com](http://www.opsware.com), or call 408-744-7770.

**About Opsware Inc.**

Opsware Inc. is the world's leading IT automation and utility computing software company. The growth of the Internet is driving a shift from client/server computing to Web architecture. With this shift comes an overwhelming proliferation of servers, networking devices and applications, creating massive complexity that makes an automated IT model a necessity. Opsware automates the complete IT lifecycle and delivers utility computing by enabling IT to automatically provision, patch, configure, secure, change, scale, audit, recover, consolidate, migrate, and reallocate servers, network devices and applications. Over 250 of the world's largest companies, outsourcers and government agencies use Opsware to deliver this new, automated model of IT.

Opsware is a service mark and trademark of Opsware Inc. All other product names, service marks, and trademarks mentioned herein are trademarks of their respective owners.

**Corporate Headquarters**

599 North Mathilda Avenue Sunnyvale California 94085 USA  
T 408.744.7300 | F 408.744.7383 | [www.opsware.com](http://www.opsware.com)