WHITEPAPER

Fighting Back Against Network Complexity

Targeting automation on four functional areas where you will gain the most advantage
Fighting Back Against Network Complexity

Targeting automation on four functional areas where you will gain the most advantage

Ironically, IT complexity is in many ways the result of success.

Business success leads to growth, and growth means more users on the network, more devices, more mobility, more complexity—and a lot more importance placed on the network.

Advances in technology such as virtualization succeed in delivering benefits like flexibility and reduced cost, but at the same time create moving parts and rapid change for network teams.

And who is at the vortex of this perfect storm of complexity? Network managers, that's who. Everything touches the network; and the more complex things get, the more complex network management becomes.

Many network teams are struggling with building more efficient and responsive organizations because of requirements imposed on them by trends and advancements in other parts of IT and in the business at large. They are faced with the need of moving from traditional approaches that worked years and decades ago to a more efficient approach to their core functions. And the key to that approach will be automation.

In almost every walk of modern life, the answer to complexity is automation.

As individuals, we have already moved away from many of the detailed and time-consuming tasks that used to make up our daily activities. We delegate chores to computerized coffeemakers, voicemail systems, electronically timed lawn-sprinklers, programmable entertainment centers, and GPS-based driving instructions. We're even starting to hear about auto manufacturers designing cars that drive themselves.

And like life in general, the function of network management is rife with repetitive processes that require too much attention, too many repetitive tasks, and too much time.

In a world of unlimited staff, unlimited time, unlimited expertise, and unlimited patience, all of these tasks could be handled manually. But that's not the world we live in.

What Today’s Network Managers Face

Enterprise networks are increasingly complex and dynamic environments with more users, more devices, greater mobility, bigger security risks, and increased use of virtualization. Thus network management is increasingly difficult, costly, and time-consuming. At a time when IT organizations are working to establish themselves as sources of innovation and business value rather than cost centers, this is especially frustrating, and it costs the business in more ways than one.
In the following pages, we'll look at how network automation can help you push back against complexity and win back time and resources that you can apply to innovation and to adding business value. We see four clear areas where network automation can address the challenges mentioned above and dramatically improve IT efficiency. We'll explain why current manual processes are often a weak link in building more efficient and responsive IT organizations, discuss a more efficient approach to discovery, compliance, security, and change and configuration, and present ways in which network automation can deliver dramatic efficiency, cost, risk-management, and reliability improvements.

A Practical Assessment of what Automation Can Do for Network Management

Let's start by pointing out that automation isn't magic. You can't simply plug it in and let it do everything for you. Much of what you do as a network manager requires oversight, expert decision making, and frequent intervention. What automation is good for is performing repetitive, consistent processes that consume time and resources—and that are often overlooked or ignored when network staffs are busy.

To get a realistic and specific idea of where automation is useful, we have to step back and look at it in the context of the trends mentioned above. In response to these trends, application and server teams have embraced automation, but many network teams are still using legacy processes—for functions that are far more critical today than they were yesterday. Network teams are being asked to do more with less, and as a result, the network is becoming a bottleneck for adding new services; highly paid expert staff members are performing basic, repetitive, menial tasks; and valuable contributions to key business initiatives are not getting made.

Based on this reality, automation is best applied in four key areas:

- Discovery
- Change and configuration
- Compliance and standardization
- Access control list (ACL) and rule provisioning

Discovery

One of the most detrimental effects of network complexity is that managers and administrators can easily lose track of what makes up the network and what's connected to it. Most organizations use some combination of manual processes, ping sweeps, freeware scanning tools, spreadsheets, databases, and Visio diagrams in an attempt to gain visibility into their networks.

The time involved and the drain on staff resources are immense, the task is never done, and at any given moment, the information available is out of date, incorrect, or incomplete. Many organizations, forced to choose between devoting resources to this inefficient effort or applying them to business-support initiatives, elect to do the minimum and hope the lack of information will not cause problems later.
A lack of continuous monitoring leads to other problems such as rogue devices on the network and increased security risks. It also leads to continuously adding switch port capacity instead of reclaiming unused ports, because no one knows which ports are truly available, or which ones might be needed later. Add the lack of visibility into field notices, product security incident response team (PSIRT) warnings, end-of-life and end-of-support dates, and expiring maintenance contracts, and all you’ve really done is shift resources from one time-wasting menial task to several others.

It is a clear situation in which automation can not only perform the task more cost-effectively, but can do it better as well.

By automating the discovery of multivendor devices, you can:

- Detect all devices connected to the network and how they connect to each other
- Alert administrators when new devices attach
- Identify unplanned or rogue devices
- Assign managed devices to domains based on criteria such as device type, vendor, location, and so forth

Your administrators can have access to rich inventory data that includes not only devices but also vendors, models, operating system versions, routes, subnets, VLANs, interfaces, redundant routing peers, and more. With automation, this information can be continuously updated, so that administrators are working with complete, up-to-date data rather than snapshots taken at different times of portions of the network.

With the added ability of delivering information in the form of topology views, it becomes much easier for your managers and administrators to visualize and keep track of the shifting components of today’s complex networks. If the data is tracked over time, then in addition to the current view, they have access to equally accurate and complete historical data for compliance, troubleshooting, switch-capacity planning, and trend analysis.

**Change and Configuration Automation**

Eighty percent of network problems today are the result of change—mistakes made while manually changing devices, poorly set configurations, inconsistent standards, unanticipated impacts on other network components, and more.

Like discovery, manual change and configuration processes consume time and resources. They also raise the issue of expertise. Making changes using command-line interfaces (CLI) or scripting is a highly specialized skill, and your organization might not have the necessary staff skill set available at the right time. Automation makes it possible to embed expertise and best practices into repeatable procedures, ensuring competency as well as conserving time and resources.

Many organizations may have some form or some degree of automation for change and configuration management—freeware for daily configuration scrapes, for instance, or vendor-specific tools that only work for a subset of the devices deployed. Most of these tools require specialized expertise, and some of them give all-or-nothing access, causing managers to choose between giving access only to the experts (and taking up too much of their time), or giving less-experienced techs
access and risking errors. In addition, the fragmented nature of these tools makes it nearly impossible to ensure all changes are documented or to identify discrepancies between the actual state of the network and the desired state.

Successful automation of change-and-configuration management, by definition, requires a single, purpose-built application for:

- Change detection and tracking
- Collection and archiving of configuration data
- Simplified configuration comparison
- Built-in and customizable tasks for common repetitive functions ranging from simple password upgrades to complex operating system upgrades
- User-based access controls

The power of automation is in delivering more capabilities to a wider set of staff while maintaining control, accountability, and auditability. Instead of relying on the expertise of a small number of staff, the pre-approved and tested tasks can be implemented quickly with less risk of human error. And by automating change and configuration you can:

- Reduce your reliance on CLIs
- Easily detect, track, and archive current and previous configurations
- Push responsibility for changes down to less-experienced staff
- Turn time-consuming common tasks into mouse clicks

**Compliance and Standardization**

Here’s what happens in most IT organizations when new regulations or standards come along. Someone researches the new requirements, attempts to cobble together actionable tasks, puts the information in a binder, and puts them on a shelf. Since everyone is busy with other tasks, no one thinks about them until there is a problem, or an audit is scheduled. Then a significant portion of the network team sets aside whatever critical tasks they are working on, manually inspects the policies rule by rule, one device at a time, one log at a time, trying to find issues, determine the state of compliance, make sure the new mandates are being followed, and prove that processes have not caused violations.

In other words, chaos and time-consuming tasks that pull staff off other critical requirements.

With the number of external mandates steadily increasing and the need for internal best practices and security standards on the rise, compliance has to be an ongoing process, not an occasional fire drill. If network teams want to prevent resource-devouring emergency efforts, reduce the risk of noncompliance and policy violations, and avoid finger-pointing between security teams who define standards and network teams who don’t have time to deal with audits, then they need to automate the processes involved in regulatory and policy requirement, and make them into ongoing functions.
Like change and configuration automation, automating compliance and standards can:

- Bring expertise to the process without tying down (or worse yet going out and hiring) staff with advanced knowledge of particular regulations and standards
- Allow rules and templates to be built into automated solutions for common standards such as PCI, NSA, SANS, DISA, and STIG as well as for company-specific policies and allowing devices across the network to be automatically—and continuously—checked for non-compliance or violations
- Utilize automated reporting to alert administrators to rule violations, identify the causes of problems, and offer remediation options as they occur

### Access Control List and Rule Provisioning

The fourth area where we recommend automation is the provisioning of access control lists (ACLs) and rules to routers, switches, and firewalls. This kind of provisioning is an inherently time-consuming and risky process. As networks become ever more complex, the number of access requests that require punching holes in network security devices is soaring, and there are usually five to seven devices along the network path that need to be changed for a single request. In addition, these devices are often from multiple vendors, so a single request can require various types of specific expertise.

As a result, provisioning requests can take days or weeks, depending on workloads. Since specific expertise is needed, the burden on the network team in terms of both labor and skills is heavy. With the complexity, size, and scope of network security devices, managers and administrators can often only hope the provisioning of a new service doesn’t negatively impact other network components. Once again, automation yields multiple advantages:

- Provisioning-related tasks such as discovery, path analysis, and monitoring can be automated, enabling network and security staff to see, clean up, and provision rules and ACLs in such a way as to protect compliance and optimize business operations.
- By leveraging embedded expertise within a platform, individual users do not need to be experts to decipher the complex syntax differences between different vendors.
- Modeling, testing, and provisioning to multiple devices can occur simultaneously.
- Automation can simplify rule and ACL provisioning, reduce risk, improve speed and efficiency, and increase accuracy.
Expect the Challenges To Get Worse—and Automate Now.

Manual procedures are already woefully inadequate to cope with the complexity of contemporary network management. If you are dependent on a mixture of freeware, vendor-specific tools, and legacy manual processes now—you will be in dire straits tomorrow. The sooner you start looking at network automation solutions, the better.

Infoblox can help you bring network management up to speed with the accelerating demands of new technology and business trends. Contact us today and learn how you can:

• Reduce the time and effort you are pouring into manual processes
• Take the guesswork out of network management by replacing out-of-date spreadsheets with dynamic discovery
• Find problems before they find you
• Maintain and demonstrate compliance without disrupting operations
• Improve capacity management and rogue-device detection by expanding your visibility to your end-point devices

About Infoblox

Infoblox (NYSE:BLOX) helps customers control their networks. Infoblox solutions help businesses automate complex network control functions to reduce costs and increase security and uptime. Our technology enables automatic discovery, real-time configuration and change management and compliance for network infrastructure, as well as critical network control functions such as DNS, DHCP, and IP Address Management (IPAM) for applications and endpoint devices. Infoblox solutions help over 6,700 enterprises and service providers in 25 countries control their networks.