WHITEPAPER

Is it time to automate your Network Change and Configuration Processes?

14 Questions to help you determine whether legacy manual procedures are holding you back

Table of Contents

Is it time to automate your Network Change and Configuration processes?

14 Questions to help you determine whether legacy manual procedures are holding you back

With networks becoming ever more critical to business success, most IT and network managers are painfully aware that legacy manual processes are a speed bump in delivering new services in the timely manner executives expect. They also know that application and server teams—empowered by automation—are spinning up new business services in minutes or even seconds while network teams can take days or weeks to make the changes required to deliver the services to employees, partners, and customers.

Automation tools are currently available to network teams as well, but even so, most network teams still use legacy techniques and tools—manual processes, ping sweeps, freeware scanning tools, spreadsheets, databases, Visio diagrams, printed regulations and policies stored in ring binders, and vendor-specific tools that only work for a subset of the devices deployed.

Why, if these antiquated techniques are causing the delivery of network services to lag behind the delivery of applications and servers, are they still in use—especially since automated alternatives are available? Perhaps it is because, as inefficient as they are, they've been used for decades and they work, more or less, as long as you have enough time, staff, and expertise. Too often, network teams are swamped with day-to-day requirements and focus on just keeping their heads above water instead of seeing what can be done to improve the situation.

So as the growth in complexity outpaces the increases in resources, it is more difficult each day to keep up. As a network expert, you have to ask yourself which will ultimately cost your business more:

- Sticking with what you have been doing and trying to endure the inefficiency, unreliability, and drain on staff resources—and passing up the opportunity to refocus expertise onto key business initiatives—just to maintain the status quo
- Or taking a new approach and evaluating network automation solutions, watching demos, mapping features to your unique needs, justifying the cost of the solution you select, and undertaking a deployment project

Based on our experience helping thousands of businesses automate network management, we've compiled this list of 14 questions to help you determine if legacy manual processes might be hindering your success, and to assist you in making a pragmatic decision about what is best for your network team and your business.

Does Any of This Sound Like You?

Without detailed knowledge of your individual network and your business requirements, this can't be an actual cost-benefit analysis, but it can give you a rough idea of what legacy manual processes are costing in terms of time and risk— and what you might gain from network automation.

Are you using spreadsheets and Visio to know what's connected to your network?

YES ☐ **NO** ☐

Legacy approaches to network visibility are both inefficient and ineffective. Network team members—often the most experienced and capable ones who could be making much more valuable contributions to business initiatives—spend hours collecting information manually, and when all is said and done, that information is likely to be out of date, incomplete, and incorrect in today's dynamic environment.

Are you constantly adding capacity rather than reclaiming switch ports?

YES ☐ **NO** ☐

If you are continually adding switch port capacity, but haven't recently reclaimed any unused ports, then you probably don't have enough accurate information about usage to be confident that reclaimed ports won't be needed later for the functions, so you leave them stagnant just in case. As a result, you're not making the most efficient use of your infrastructure.

Do you track field notices and product security incident response team (PSIRT) warnings via email and/or rich site summary (RSS) feeds?

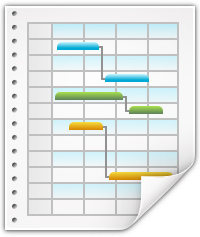
YES ☐ **NO** ☐

Lack of visibility into field notices, PSIRT warnings, end-of- life and end-of-support notices, and the expiration of maintenance contracts puts you at risk of security gaps on your devices. Email and RSS feeds are reactive, requiring someone to track the notices and then decipher how each might or might not impact the different models and operating system versions of all the devices.

Do you use command-line interfaces (CLIs) to make changes to routers and switches?

YES ☐ **NO** ☐

Because CLIs require specialized skills, they limit the number of networking staff that can make changes, which is inefficient and can cause a single point of failure in the change process. Since CLI requires touching devices manually, the risk of human error such as transposing characters on the keyboard or messing up a copy-and-paste function from a separate spreadsheet is greatly increased.



Are you unsure whether every change is made using established processes and is documented?

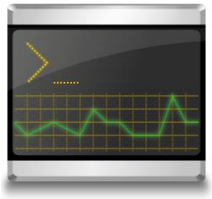
YES ☐ **NO** ☐

In an ideal world, all changes should go through a change-management process and be fully documented. In the real world, changes are often made outside the process and are missing documentation—which adds security risks, increases compliance violations, and lengthens the time it takes to troubleshoot network issues. If you don't know a change happened, how do you document it?

Do you have one or two key people who write custom Perl scripts?

YES ☐ **NO** ☐

If your organization depends on one or two experts to do complex work like writing Perl scripts, then your overall effectiveness is at risk. Because of their expertise, they're likely to have to leave one task to help with another, causing delays. And if they leave the organization, it's virtually impossible to transfer their institutional knowledge to remaining team members before they go.



Are you using vendor-supplied tools for managing network devices?

YES ☐ **NO** ☐

Because vendor-supplied network change-and- configuration tools are often included with purchased equipment, network teams tend to use them at first. But the organization eventually ends up with multiple tools for managing routers and switches, and dealing with changes still requires extensive, vendor-specific expertise. As complexity increases and business demands rise, these supposedly free tools, which are kept in use mostly by inertia, place an increasing burden on staff and an increasing drain on efficiency.

Does your existing network team need to complete audits for external compliance or internal security requirements?

YES ☐ **NO** ☐

Most businesses have to comply with external regulatory mandates such as PCI, HIPAA, and SOX, and as security threats become ever more dangerous, businesses are also putting stringent internal security policies in place. Regulations and policies mean audits, and if your network team has to respond to them by creating a task force to manually collect, tabulate, analyze, and present data, it means time taken away from delivering network services to support the business.

Do your security and network teams occasionally come into conflict?

YES ☐ **NO** ☐

Translating security best practices into actionable network requirements can be difficult. The security team wants proof that the policies they've devised to protect the business are being followed. The network team is busy with a hundred other things. The result is often confusion, hostility, and blamestorming.

Do you focus on compliance only when audits are due?

YES ☐ **NO** ☐

If so, you are being doubly inefficient. Audit response is draining major resources away from important work, and the results obtained are usually inadequate because reactive information gathering and analysis take place too quickly to be accurate and complete. Compliance should be a continuous and ongoing process, not a periodic event— accomplished not by massive application of manpower, but by automation.

Is the number of service requests that require ACL and rule changes growing?

YES ☐ **NO** ☐

A spike in the number of service requests means a spike in the number of changes needed to punch holes in routers, switches, and firewalls. For the vast majority of organizations, the growth in staff and budget resources is not keeping up with the growing dynamic requirements.

Do most service requests require changing three or more network devices?

YES ☐ **NO** ☐

Not so many years ago, responding to service requests was fairly simple, because a single request involved punching a hole through a single firewall. Today, the typical request includes many devices including firewalls, routers, and switches. On average, each change touches between five and seven devices. With different vendors for routers, switches, and firewalls, the impact on the team grows exponentially.

Are your change-request service-level agreements measured in days or weeks?

YES ☐ **NO** ☐

If they are, the network team just might be squandering the rapid response that application and server teams are delivering. While those teams are spinning up new services in a matter of minutes, the network team is spending days or weeks to provision the network—and IT in general is unable to meet business expectations.

Are your budget and staff strained by growth in demands and requirements?

YES ☐ **NO** ☐

Part of the reason is growing complexity, criticality, and demand. But it is probably also the result of using legacy manual processes that can't scale in response to the increasing challenges IT faces. If more than half of your day is spent troubleshooting or on unplanned tasks that just happened to pop up, you understand the pain of continuing the same approach as the networking world is rapidly changing.

If You're Not Ready to Automate Now, You Will Be— Because Complexity Will Continue to Increase.

Just take a look at the checklist, and see how often you answered "yes." The more times you did, the more automation can help you move away from what you have been doing to what you should be doing. If you conclude that you're not quite there yet, complexity and growth will catch up with you sooner or later. So why wait? Get started today by exploring a network automation solution that can keep pace with today's rapidly changing network environment. Our industry-leading multivendor network automation solution includes tools for:

- Automated discovery that can tell you exactly what's on your network; switch- port analysis to track what is free, used, and available to be reclaimed; and integration with Cisco deployments to reduce security vulnerabilities
- Change and configuration management that reduces your reliance on CLIs; automatically detects, tracks, and archives current and previous configurations; includes prebuilt tasks and customizable templates; and supports the majority of common network-device vendors
- Compliance and standardization that leverages embedded expertise and customized rules to ensure compliance with external and internal mandates and turn security policies into actionable network requirements; continuous monitoring; and single-click reporting
- ACL and rule provisioning that applies intelligent automation to common repeatable tasks; analyzes, defines, and provisions to one or many devices simultaneously; and centralizes provisioning task management to reduce the risk of errors and the time and expertise needed to implement changes

In short, Infoblox can help your network team get up to speed with the accelerating demands of new technology and business trends.

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com