UPLOGIX

WHITE PAPER

TAKING NETWORK MANAGEMENT LOCAL TO ENABLE *REAL* AUTOMATION

EXECUTIVE SUMMARY

Despite decades of advancements in network speed, reach and security, the management of network devices is still a hands-on task. It involves reactive and often tedious actions open to human error. Traditional Network Management tools rely on the network itself to manage critical devices. This dependence on the network to manage the network is a critical design flaw. It limits the levels of automation administrators are willing to apply and ensures that when problems occur, those management tools offer little value.

One strategy to solve this design flaw is to de-centralize the management of network devices by connecting directly to devices and create an alternate path or network-independent connection. This approach can eliminate the roadblock while increasing network reliably and security. Also, many of the routine administrative tasks that consume a large portion of time can be automated. This local management strategy can free up time and resources that could be spent on innovation and improvements, instead of just "keeping the lights on."

CONTENTS

Network management remains a hands-on activity. And so are errors – 80% or more of network outages are due to people and process issues.

THE NOC AS YOU KNOW IT: CENTRALIZED NETWORK MANAGEMENT TOOLS

Network management tools have traditionally been a centralized set of applications that collect and organize information about the devices connected to the network and provide a comprehensive view of the state of the managed environment. Sophisticated management systems pull together vast amounts of data, arranging it clearly and helping IT groups assign tasks and manage their networks.

Gartner has stated for years that upwards of 80% of network outages are a result of human and process errors. Yet network management strategies remain highly hands-on. All centralized tools face the same major limitations because they rely on the network to gather data and connect network administrators with the gear they need to manage. As a result, there is a very real risk that when these tools are needed the most, during an outage or failed configuration change, they will be useless.

With this shortcoming in mind, few are willing to enable meaningful management automation. Even as other aspects of network management have advanced, centralized tools support IT, but don't actually remove the burden of time and effort with *real* automation.

THE REQUIREMENTS FOR DE-CENTRALIZING NETWORK MANAGEMENT

TAKE THE NETWORK OUT OF THE CRITICAL PATH

As we have observed in the transitions and evolutions of the centralized computing and distributed computing models, the solution for network management automation lies in deploying some intelligence where it's needed. Locally—out of the NOC and into the rack with the gear needing management. A local management platform connects over the console port (like a technician with a crash cart), and the dependence on the network itself can be removed from the management path.

The console connection is the most basic level of interaction with a device. Utilizing a command line interface (CLI) also makes it possible for a unified common interface to manage heterogeneous network devices and servers.

INTELLIGENCE AT THE EDGE

With a secure console connection established, the next step is to add local processing and storage, ensuring independence from centralized applications. This enables continuous monitoring at a much higher resolution than traditional management standards. For example, in order to reduce the amount of management traffic on the network and load on devices, many centralized tools poll devices every 15 minutes—or even longer periods. This impacts SLAs and user experience, yet is generally considered an industry standard.

By connecting directly to critical network devices, congesting traffic created by centralized polling solutions can be avoided. Since the connection is over the console,

the devices' networking operations aren't taxed either. Decisions about default sampling times can be reduced from how many times an hour to how many times per minute, and more extensive data can be collected. In addition, since data isn't collected over the network, in the event of an outage device data continues to be collected, providing vital troubleshooting and security accounting information.

All of this data needs to be stored and analyzed locally—removing the need to ship data to centralized tools for processing. This not only means more rapid detection of issues, but also the ability to store information for trend analysis and batch archiving at a later time. Being able to trigger automated actions based on trends avoids "knee-jerk" responses.

Most IT groups have standard procedures based on a detected issue—responses start at the most basic and least disruptive actions like clearing an interface or cycling power, and move up to more involved operations like recovering a device in ROMmon or reloading a configuration. The recovery actions and order are pre-scripted, which is a key component for automation. Standard responses conducted by an administrator are also a key contributor to human error. Routine actions lead to taking shortcuts, which can lead to bigger problems like mass outages and security holes.

OUT-OF-BAND ACCESS

An out-of-band connection allows for the local manager to both connect to the NOC and backfill centralized tools with information.

Another key component of a local management is the ability to connect to/from the NOC if the primary network is down. Short of a power failure, during an outage most devices are likely to still be working, including the local management platform. An out-of-band connection allows for both the local manager to connect to the NOC and backfill centralized tools with information, but also for experts in the NOC to access remote gear for more challenging repairs.

The distributed nature of critical network infrastructure today requires flexibility when it comes to the type of out-of-band connection. Options are needed for POTS lines (often readily available, and fast enough for CLI interactions), cell modems (great as a low-cost, easy-to-install solution with fairly high bandwidth potential), secondary Ethernet connections (using alternate network systems), or even satellite links (for especially remote or mobile sites).

SECURITY

As a gateway to devices, a local management platform needs to be highly secure from a policy enforcement standpoint as well as audit and compliance reporting. Under normal operations, the local management platform can authenticate through standard mechanisms like TACACS and RADIUS, but even if connectivity is lost, it should be able to failover to other AAA servers or fall back on cached authentication data.

Data on the device should be encrypted in accordance with a stringent certification like the Federal Information Processing Standard (FIPS) publication 140-2. Levels of this standard include physical security specifications, ensuring both hardware and software components are secure.

In most industries, automation is the norm. Network management has long been an exception due to the reliance on the network to manage the network.

Leveraging the dedicated serial connection to managed devices, the local management platform is in position to log all changes made by users and the results of the changes. This information can be saved locally, and then archived in a central location for deeper analysis and long-term storage. This compliance reporting is resilient and occurs when the network is up or down.

THE BENEFITS OF A LOCAL MANAGEMENT PLATFORM

With these components in place, key challenges to more effective network management are addressed by putting select functionality where it is needed the most—right where the managed devices are.

RELIABLE AUTOMATION

In most industries, automation is the norm. Network management has long been an exception due to the reliance on the network to manage the network. Once you remove this weakness, it's possible to focus on bigger issues. Real network automation isn't just about knowing there is a problem to fix, it's knowing that the problem was already fixed for you.

Best practices and runbook procedures are followed each and every time. Using the high-resolution monitoring data, automated responses are taken to device issues, saving time and service calls. For example, say a router drops in ROMmon mode. It is detected within 30 seconds and recovery begins. Automatically power is cycled to the router and the local management platform locates the device's boot file or loads a new image from the last known good image stored locally on the platform. At the appropriate time, the boot command is issued pointing to the correct file and the device resumes normal operation.

Mass configuration changes on like devices can be scheduled and executed as batches, rather than an administrator updating each device one by one. This automation not only saves time and effort, but also removes opportunity for human error. This combination of time, effort and risk leads to the common delays of maintaining security patches and updates.

The added capability to automatically roll-back configuration changes makes it safe to apply changes and updates often, ensuring new threats are addressed immediately as they become known.

When a device has issues, they are detected and trigger the appropriate runbook responses. Dashboard and ticketing devices can be alerted of the issue and provided with a full account of steps taken. If problems remain, IT staff doesn't have to start at the beginning of the problem solving chart because they know exactly which device has the problem and that initial steps have already be attempted, which means less time and effort.

SECURE, TWO-WAY REMOTE ACCESS

By providing persistent connectivity to network devices the NOC has management access and control to distributed gear, even when the network is down or degraded.

As an onsite toolbox, a local management platform can support IT operations with secure remote connections, local storage and automated functionality. For example, sometimes devices fail and need to be replaced. Previous configurations are pulled and stored automatically for managed devices, which means that a "bare metal restore" is possible. A replacement device is cabled in place of the broken device, and the local management platform can push the previous configuration, bringing up the new device. This support takes some of the burden off the IT worker—speeding up the process and lowering the level of skill or training needed to perform the job.

In the heat of the moment when network problems arise, urgency can prevail over security… this is precisely the circumstance that sets the stage for a serious breach, unintended or not.

TIGHTENING INFRASTRUCTURE SECURITY

Local management addresses two forms of critical security vulnerabilities that continue to plague mission critical network infrastructure and account for the majority of related security breaches.

Network devices that cannot be frequently and easily configured and upgraded cannot be secured. "If it ain't broke don't fix it" is a hacker's dream. Automated support makes it easier to update the software and configuration of network and communications devices in the face of constantly evolving security threats. Whether that is mass updates backed up by the automated roll-back of failed configurations or securely updating access passwords on hundreds of managed devices in a single action, a local management platform reduces the routine tasks that are the source of many security issues.

In the heat of the moment when network problems arise, urgency can prevail over security. Break-glass root passwords are issued to empower technicians to console connect to devices and resolve issues, any centralized administrative audit is off-line, and carefully crafted policies intended to protect data are quickly forgotten. This is precisely the circumstance that sets the stage for a serious breach, unintended or not.

With a console connection to managed devices, a local management platform simultaneously enhances a technician's ability to mount an effective response to issues while ensuring that security and audit are not compromised. By storing encrypted device credentials only on the local platform, secure, policy-compliant and audited administrative access can be ensured with complete logging of all transactions for compliance requirements.

MAKING CENTRALIZED MANAGEMENT TOOLS STRONGER

A local management platform doesn't replace traditional tools; it removes the fundamental weaknesses that have limited real network automation for years. The device-level data used by traditional centralized management tools includes device statistics collected via ICMP, SNMP get requests and SNMP traps based on predetermined thresholds and rules. These tools gather and receive this important

information from devices over the network. If the network isn't available, the data isn't either, and centralized network management cannot do its job.

With a local management platform that device-level data keeps flowing even if the primary network is temporarily unavailable. Device statistics and SYSLOG messages can be collected directly via a device's console port. This information is stored locally and delivered at regular intervals to the NOC and forwarded to centralized tools where it can be used to replace or augment statistics that might be missing or incomplete. Traps can even be forwarded over an out-of-band link to centralized tools when the network isn't available. Instead of dashboards reporting that every device at a remote site just went down, administrators have actionable data for remote sites that lets them work on the problem, not just working around the problem trying to isolate it.

MEETING THE INCREASING DEMANDS ON THE NETWORK

Cloud, the Internet of Things, BYOD, M2M… Just about every story in IT these days involves placing a greater burden on corporate networks. One of the many concerns is the increasing demand on IT to deliver these critical networks. Network management remains so hands-on because of the risk involved in using traditional tools for any automation that requires the network to manage the network.

By deploying network management locally—in the rack with devices like routers, switches, firewalls, etc.—reliable automation is possible because the management is done out-of-band, independently of the network.

The benefits of reliable network automation include less time spent by IT staff on routine tasks, decreased opportunities for human error, increased uptime, and tighter security. All areas key to delivering on the expanding expectations for the networks of today and tomorrow.

For more information about local management, please visit **uplogix.com**. Uplogix provides the industry's first local management solution. Our co-located management platform automates routine administration, maintenance and recovery tasks—securely and regardless of network availability. In comparison, traditional network and systems management depends on the network, uses multiple tools, and remains labor intensive. Uplogix puts the power of your most trusted IT administrator everywhere, all the time.

Uplogix is privately held and headquartered in Austin, Texas.