EXECUTIVE EDITORIAL

MEETING IT CHALLENGES IN A DO-MORE-WITH-LESS CLIMATE

WHY RELIABLE NETWORK MANAGEMENT AUTOMATION IS CRITICAL IN AN AGE OF SHUTDOWNS, SEQUESTERS AND BUDGET CUTS

By James Dollar, Uplogix Founder and CTO

It's a tough time to run an IT group in a governmental agency. The services IT provides are more critical and pervasive than ever and user expectations have never been higher. Add to that the demand for efficiencies and cutting costs is ever-present.

There are options. The cloud promises economies of scale and as-needed availability. Data center consolidation provides savings and simplification after a decade of expansion. The trend toward centralization of applications and services makes the network even more critical.

When it comes to providing faster, stronger networks, network management tools are getting better, but only incrementally because they still rely on trained humans to actually do most of the work. Real network management automation hasn't taken off because of the basic issue that tools are still dependent on the network to manage the network. As a result, they are pretty much limited to reactive tasks like monitoring, dashboarding and analysis.

Until IT groups move beyond this fundamentally flawed approach, they won't be able to realize automation savings and just "keeping the lights on" for the network will continue to consume upwards of 50% of IT's resources. By de-coupling the management of the network from the network itself, great gains can be made toward reducing the human effort required while providing the resilient networks needed for the success of cloud and other cost saving initiatives.

WE'RE MOVING TO THE CLOUD AND CONSOLIDATING OUR DATA CENTERS, ISN'T THAT THE ANSWER?

Cloud computing and the consolidation of data centers clearly have direct economic benefits of centralizing processing and storage. However, it does make the network

more critical to ensure access to the cloud and the applications in it, driving higher requirements for network performance and availability.

Legacy thinking considers the network merely plumbing. With cloud computing, success is highly dependent on the network—the cause of users' cloud frustrations might actually be caused by a trickle of data flowing through a troubled network. Business and IT leaders must position the network as a strategic asset that will determine the ultimate success or failure of cloud services. For every network device, service level requirements are higher and there are more devices to deploy, configure, monitor and troubleshoot. Without changes in the network and how it is managed to anticipate all of this, there are two options. One would be that the network will swiftly become the weak link in the chain and cloud initiatives will fail. The other is that attempting to keep up with network SLAs will drive an increase in spending for IT staff to better monitor and respond to issues.

Few at the executive level would argue that shifting expenditures from one column to another is true progress. So how do you deploy the network infrastructure you need without breaking the bank and losing the cost savings you realized from moving to the cloud in the first place? First you have to look at where the money is going.

THE HIGH COST OF PERSONNEL IN IT

For years, one of the standard industry stats is from Gartner, saying that 60% of total worldwide IT expenditures go into IT infrastructure and operations (I&O). Gartner goes on to say that I&O accounts for about 50% of total IT headcount, with most involved in day-to-day and tactical operational processes. When it comes to managing networks, many of these talented professionals are spending their time on routine maintenance. When there are issues in remote networks, the solution is a truck roll, just get someone out there to see what's going on. Whether outsourced or fielded by internal staff, onsite troubleshooting is slow and expensive.

Another related cost of all of the human involvement in network management is security. People are the cause of most security breaches. They skip steps tying to save time and get distracted and leave tasks undone or done incompletely, introducing vulnerabilities into the network. Using a machine to automate some of the basic network management tasks means that jobs are going to happen the same way every time. Exactly like the run book says to do it.

DOING MORE WITH LESS, THE DEFINITION OF AUTOMATION

The reason why network management is so hands-on is because of the risk involved in using traditional tools to actively DO the work versus passively reporting status and providing assistance tracking changes. Automation is impractical when it can break your network and leave you cut off from the devices in trouble.

Limitations in management software also typically require homogeneous platforms to operate. That's a high bar in today's environment where it's common for organizations to merge, leaving IT groups to figure out how to manage disparate networks. This leads to fractured organizations that maintain a less-efficient "separate, but equal" approach to running the network.

So what's the answer? First you need to accept that the root cause of the limitations—managing the network over the network—is not the most efficient way of doing business. By deploying network management locally, that is in the rack with devices like routers, switches, firewalls, etc., reliable automation is possible because the management is done out-of-band, independent of the network.

IT'S LIKE A VIRTUAL ONSITE TECHNICIAN

The console port is a connection on a device designed to be used by technicians for setup and troubleshooting of devices. Connecting a virtual IT technician to it has some clear advantages:

- Continuous out-of-band monitoring – Polling of devices can be much more frequent and gather more data than what would be done across the network. This means issues are known and the source pinpointed faster.
- Automated support – with onboard intelligence to store polling information as well as processing and a rules engine, level-one run book responses can be automated. These make up the bulk of issues IT staff deals with today: routine problems with routine solutions. These tasks are prime for automation if you can have confidence in the tool.
- Configuration and change management – Stage changes for similar devices across the network and push them automatically with the confidence that any devices with failed changes will automatically be rolled back to the previous working state.

REMOTE ACCESS

The next aspect of a local management platform is accessibility. Say the network is down and the problem is beyond the automated capabilities. At this point, you want to put skilled humans on the task to deal with an unusual situation. The platform needs an integrated out-of-band connection, typically a phone line, cell modem or a secondary network that ensures experts in the NOC can access gear as if they were onsite.

This connection can also be used to feed data upstream to centralized tools. Traditional polling might be down, but the local management platform can forward device status into the dashboard and reporting tools already in use.

THE KEYS TO THE KINGDOM

What about security? It's one thing to have confidence that the solution will do the job, but is it secure? A local management platform is built around secure processes. From encrypted communications, configurable role-based access, to AAA caching, and

complete network independent logging of all user interactions, security is a key piece of user confidence.

Don't forget that taking people out of routine maintenance situations is a good thing. A recent study by security solutions provider Symantec concluded that employee mistakes lead to nearly two-thirds of data breaches. Even when employees are not acting maliciously, their actions can cause major security problems. Limiting their opportunities for error is a good idea.

WHEN THE GOING GETS TOUGH…

The tough have to look for smarter ways of getting the job done. Reining in data center expansion and moving storage and applications up to the cloud are clear strategies. Unfortunately, as with most game-changing solutions, new vulnerabilities are exposed. In this case the reliance on the network to access the cloud effectively will make an already stretched element even tougher to manage without massive escalations in cost for support. Unless you start managing smarter.

To lower costs without giving up capabilities, or even provide stronger networks, management automation is required. For this, a new approach is needed that counters the weakness of decades of network-dependent, human-intensive management. The answer is to deploy intelligent network management where the gear is—in the rack, connected locally and accessible remotely and securely. Without it, the best laid cloud plans might just rain on the IT parade.

About the Author

James Dollar is a respected technology innovator with 20 years experience designing and managing network communication infrastructures. Before founding Uplogix he was a key network architect at several application service providers, responsible for 99.999% application and network availability. Mr. Dollar has spent over a decade with world-class organizations such as The Coca-Cola Company and Reliant Energy, driving key aspects of technology and network architecture strategies. Mr. Dollar received his BBA from Stephen F. Austin State University.

About Uplogix

Uplogix is a network independent management platform that is located with – and directly connected to – communications and networking devices. It can stand alone or augment your existing centralized management tools to provide automated configuration, performance and security management functions that are best performed locally.