ActualTech Media

zpe®

The Role of Out-of-Band Management: Today and into the Future

Ed Tittel

CONTENTS

IN THIS PAPER

Out-of-band management (OOBM) uses connectivity separate from normal network connections to monitor and manage network devices. Increasingly, automation plays a key role in OOBM, to support network troubleshooting, provisioning, and configuration tasks.

ZPE Systems offers a new level of network management with a software-defined, vendor-neutral solution that brings innovation to OOBM.

Out-of-band management (OOBM) keeps data centers, remote locations, branch offices and cloud-based services running—even when people aren't present where things are happening. By using an alternate communications path rather than the primary network, OOBM provides a way to access failed devices even when the network goes down. This enormous benefit is why IT security auditors, admins, and network engineers have such high regard for OOBM.

OOBM Continues to Evolve with Wireless Connectivity

Wireless telephony is already in use in modern OOBM, with some implementations making use of 4G Long-Term Evolution (LTE) links. These can deliver speeds of up to 600 Mbps, however, new generations such as 5G and even 6G are coming into use. These offer speeds of up to 5 Gbps (with planned increases in the future), allowing for newer OOBM solutions to take advantage of higher bandwidths and deliver new capabilities.

Automation Helps Organizations Streamline Processes

Automation helps modern IT meet demands by automating and streamlining important processes. With an ever-expanding need for information services, automation will play an even bigger role in OOBM. As infrastructures become more complex with "SD everything" coming into play, it's vital for any organization to automate as much as they can.

As a start, things always get done right when organizations automate basic repetitive configuration and management tasks in network infrastructures. In fact, automation takes time-intensive manual effort out of tasks from onboarding new employees to managing virtualized IT environments. The former includes setting up accounts, provisioning phone and desktop resources, and establishing proofs of identity and authentication and related permissions for access controls. The latter includes one-offs or pilot installations for testing and early adopters. It also includes regular instantiations of Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) runtimes. That helps organizations meet specific project needs, handle peak demands, and so on. Automation works as well through OOBM as it does through direct in-band network connections.

Automation helps relieve staff of manual effort for routine IT tasks like backups and restores, archiving, logging, patching, and updating. IT teams can tackle complex or strategic jobs by using automation that helps monitor and manage critical processes. In fact, automation in IT extends well beyond virtualized environments. In the data center, automation provides real-time status monitoring of physical and logical devices. With regard to security, automation reacts more quickly and accurately than humans, allowing for immediate detection of potential exploits or other threats.

> Because automation removes constant and repetitive input at the command line or through other interfaces and tools, it speeds up development, reduces human error, and improves the IT work experience.

Because automation removes constant and repetitive input at the command line or through other interfaces and tools, it speeds up development, reduces human error, and improves the IT work experience. Better still, automation enables IT staff to devote more time to researching and innovating. By boosting productivity, automation also helps to reduce capital and operating expenses in IT (CapEx and OpEx). **Figure 1** shows Gartner Inc. assessments of enterprise planned engagement with and investments in network automation.

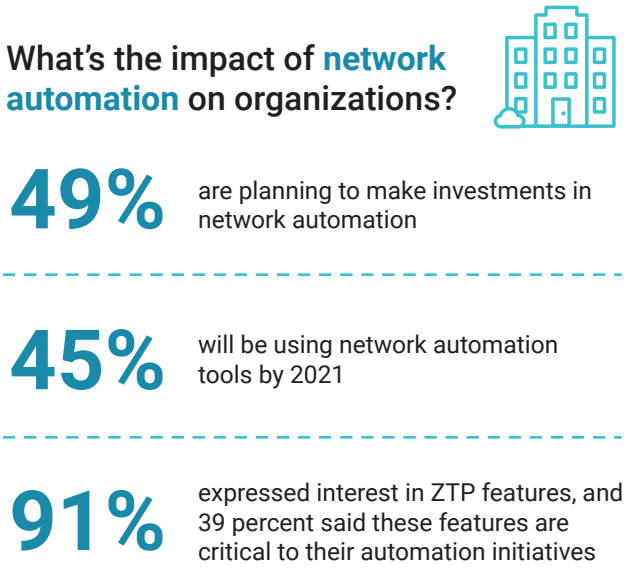

Figure 1: Organizations are moving strongly to embrace network automation, with profound interest in Zero Touch Point (ZTP) automation features (*Source: Gartner Inc. & EMA*)

PRIMARY DRIVERS AND BENEFITS FOR NETWORK AUTOMATION

Automation offers significant benefits to organizations that use it effectively and well. Chief drivers and benefits include the following:

- **Lower Costs:** Automation simplifies infrastructures through codified instantiation, modification, and maintenance. It increases efficiencies through well-tested, error-free tasks and workflows. Automation also shortens deployment times by eliminating repetitive manual tasks and completing tasks faster.
- **Improved Business Continuity:** Automation helps organizations deliver higher levels of service with greater consistency across locations. Automated monitoring and alerting mean that failures can be detected proactively and break-fix maneuvers completed before users even notice any issues.
- **Greater Insight and Network Control:** With simple changes to input parameters, automation tools help organizations adapt to changing network needs. At the same time, automation of related monitoring and management delivers improved visibility and enhanced controls to the IT staff.
- **Greater Business Agility:** Automation speeds time-to-market thanks to shortened time frames when deploying new applications and services. This means improved first mover advantages and boosts returns on technology investments.
- **Reliably Ensured Compliance:** Standard methods of deployment mean little or no variation in end products. Testing and vetting prior to production deployment help automated tasks and workflows ensure and enforce unified policy management and compliance regimes. If automation is done right up front, it stays right.

AUTOMATION FACILITATES AUTONOMOUS NETWORKING

Autonomous networking assembles piecemeal task and workflow elements via automation to produce a continuous, highly automated IT lifecycle. In such an environment, automation elements can observe, analyze, and improve actions in real time (or near-real time). As an added bonus, this requires little or no direct human intervention. Thus, automation keeps IT humming at the speed of technology.

In an autonomous networking environment, automation delivers improved consistency, efficiency, security, accessibility, and performance. When automated, functions engage more quickly and with better precision than equivalent manual activities. For example, such a regime enables load balancing and provisioning functions to react to network demands as they occur, in real time.

> In an autonomous networking environment, automation delivers improved consistency, efficiency, security, accessibility, and performance.

In general, network automation supports programmatic behavior for network activities. These activities can then accommodate the scope and scale necessary to support data-intensive and resource-intensive projects for artificial intelligence and machine learning (AI/ML), the Internet of Things (IoT), complex data analytics, and more. All of these emerging technologies benefit greatly from the

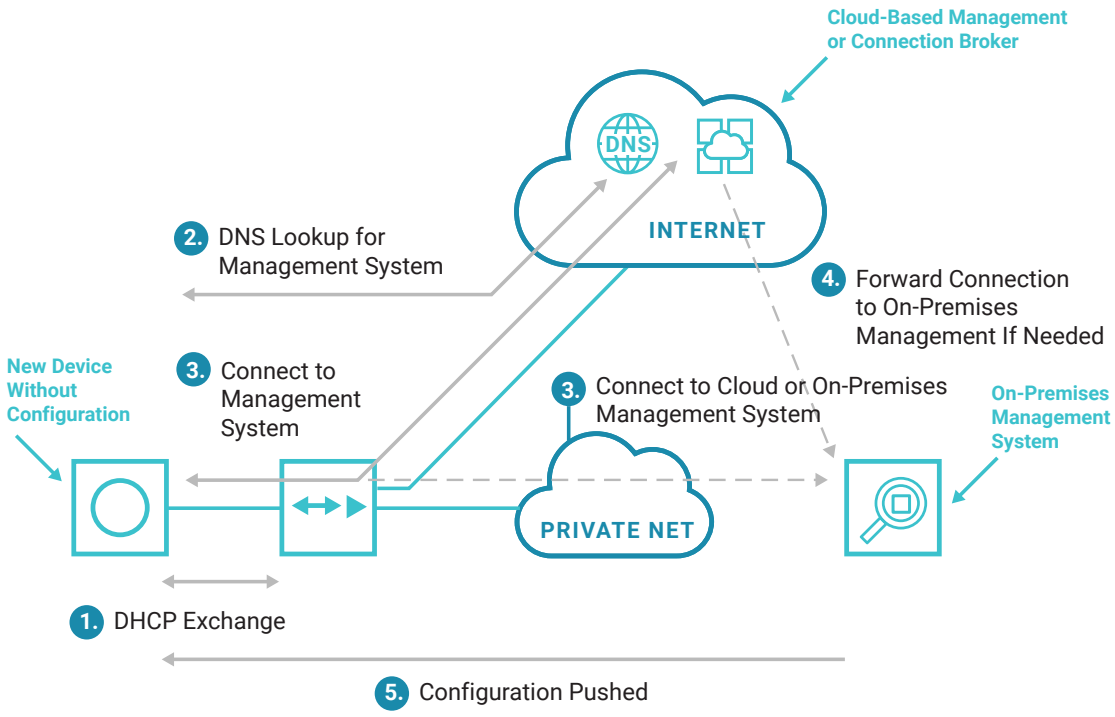

Figure 2: How Zero Touch Provisioning works

adaptability and flexibility that intelligent automation and autonomous networking can provide.

Furthermore, such automation and autonomous networks work well with Puppet-based or Chef-based orchestration capabilities. ZPE supports Ansible-based and RESTful API-based applications, as well. These can even include natural language-assisted search capabilities that help administrators and developers interact effectively with the OOBM environment and its labor-saving automation.

Zero Touch Provisioning Leads to Consistency and Scalability

One area where automation is particularly useful is Zero Touch Provisioning (ZTP). ZTP permits network devices to be configured automatically, using well-tested and well-understood scripts that incorporate specific input parameters for customization and localization. As the name suggests, ZTP greatly reduces or eliminates human touch points. It offers greater speed and accuracy than human interactions via a command line or a GUI interface.

ZTP's biggest advantages include not only speed and accuracy, but also scalability. Running well-tested scripts delivers a consistent, reliable configuration every time. Programmatic operation also means that provisioning can occur in parallel on as many devices requiring configuration, provisioning, or updating as needed, all at the same time.

> Organizations that invest the ounce of preparation necessary to achieve the pound of cure that automation provides are setting themselves up for success with greater efficiency, accuracy, and security.

To work its magic, ZTP requires development and testing in the lab before deployment onto production networks. ZTP's speed and accuracy come from comprehensive advance preparation, which often includes experimentation or trial-and-error learning to get the automation scripts and tools working just right during preliminary phases. Then, ZTP is typically deployed in data centers. However, certain cloud technologies (like those ZPE offers) now allow ZTP to be deployed over the WAN to remote locations and branch offices, extending the same benefits into locations outside the data center (**Figure 2**).

Organizations that invest the ounce of preparation necessary to achieve the pound of cure that automation provides are setting themselves up for success with greater efficiency, accuracy, and security. ZTP offers the same advantages to OOBM that it does to in-band management and workflows.

Enforce Security with a Strong, Secured Gateway

For best security results administrators need to present proper credentials and proofs of identity before they get OOBM access or use OOBM tools and facilities. In addition, OOBM activities and data must be strongly encrypted when in motion and while at rest using TPM, SSL VPN, IPsec, and modern firewalling techniques. Ideally, OOBM communications and data should be completely opaque to all unauthorized parties.

For added protection, OOBM scripts and tools should be subject to system configuration checksums generated in advance, then checked upon receipt for exact matchups. This avoids man-in-the-middle attacks that could alter or impersonate valid, verified configuration data and automation tools.

Enforce Compliance and Auditing

In the OOBM world, a single point of administrative control allows authorized administrators to incorporate policy compliance checks and measures into the OOBM environment. Automated reporting, logging, and tracking work constantly to document activities and provide forensic evidence of policy adherence and compliance with legal, regulatory, or policy-based activities and controls.

Thoughtful OOBM design and implementation help establish initial compliance. Thereafter, audits and after-action incident reports can ensure ongoing compliance. These audits and reports can be tied to policy-driven security and compliance checks, testing, and incident-handling. The result is an audit-ready, highly compliant IT environment.

Help with Monitoring System Health

By its very nature, OOBM uses communication channels outside the usual network infrastructure. OOBM is called into play when communication outages or failures require alternate methods of contact and control over networked components and other connected devices.

OOBM also provides access to network and system monitoring information, including visibility into various metrics for health, performance, and uptime. Administrators can check and interrogate network devices, understand patch levels and licensing data, observe security and incident information, and more. OOBM provides a consistent and coherent view of network health, stability, and performance that helps administrators provide the best possible service to their clients and users.

Put OOBM, Automation, and Autonomous Networks to Work

With the considerable advantages an OOBM solution can deliver to your organization, it is essential to find a technology partner or solutions provider who can help you select the OOBM solution that best meets these needs.

One such partner is ZPE Systems, whose software-defined, vendor-neutral Nodegrid OOBM system offers outstanding infrastructure management and networking controls. It not only includes a powerful OOBM experience, but also brings automation and autonomous networking to the forefront. ZPE's Nodegrid family of products and services deliver secure, comprehensive remote access via OOBM to your systems and infrastructure, keeping you online in even the toughest situations.

When you're ready to put the benefits of OOBM to work, visit the ZPE Systems website or request a demo today.