ActualTech Media

zpe®

Out-of-Band Management 101

Becky Elliott

CONTENTS

IN THIS PAPER

Are your administrators having to remember a laundry list of commands specific to each device on your network to monitor and manage them? And has the number of devices in your organization blown up beyond your control?

This tech brief explains the benefits of out-of-band management and how it provides higher-level, aggregated, and remote Access and Control capabilities for many devices from a single management point. Find out how ZPE Systems can help your organization regain oversight of networking, compute, storage, and smart power assets, regardless of who the vendor is.

During a security assessment the auditors will always ask this one question: "How do you manage your devices?" The answer should be: "out-of-band management."

> OOBM supports an organization's business continuity goals by allowing them to start troubleshooting sooner, regardless of where their hardware is located.

What is out-of-band management (OOBM)? OOBM allows you to connect to devices via an alternate path that's disparate from the in-band network, whereas in-band management relies on connecting to devices via telnet, Secure Shell (SSH), or Remote Desktop Protocol (RDP) from within the local network on which the hardware lives.

OOBM provides higher-level, aggregated, and remote Access and Control capabilities for multiple devices from a single management point. From this OOBM, you can install an operating system and remotely troubleshoot via a console.

Why do auditors love OOBM? OOBM supports an organization's business continuity goals by allowing them to start troubleshooting sooner, regardless of where their hardware is located. Quicker resolution times lessen an outage's impact on the business. Auditors also love when organizations use OOBM to harden their security posture by segregating all device management from their in-band network traffic (see **Figure 1**).

Organizations love OOBM because of features like lights-out monitoring (LOM), which allows them to check health status and configurations on those devices. Want to check a device's power status or chassis state? How about configure boot devices, or check versions of software or firmware? LOM enables you to complete those tasks and find outage-causing failures sooner. They also love the remote console because because it allows them automate commands and collect logs for auditing and monitoring.

UNIFIED MANAGEMENT

Part of the real value that OOBM brings is simplifying device management and administration in a secure manner. Managing more than 10 devices becomes unscalable quickly, and most organizations have orders of magnitude many times more.

These devices support a mixture of native interfaces: RS232, RJ45, USB, Ethernet, and virtual interfaces.

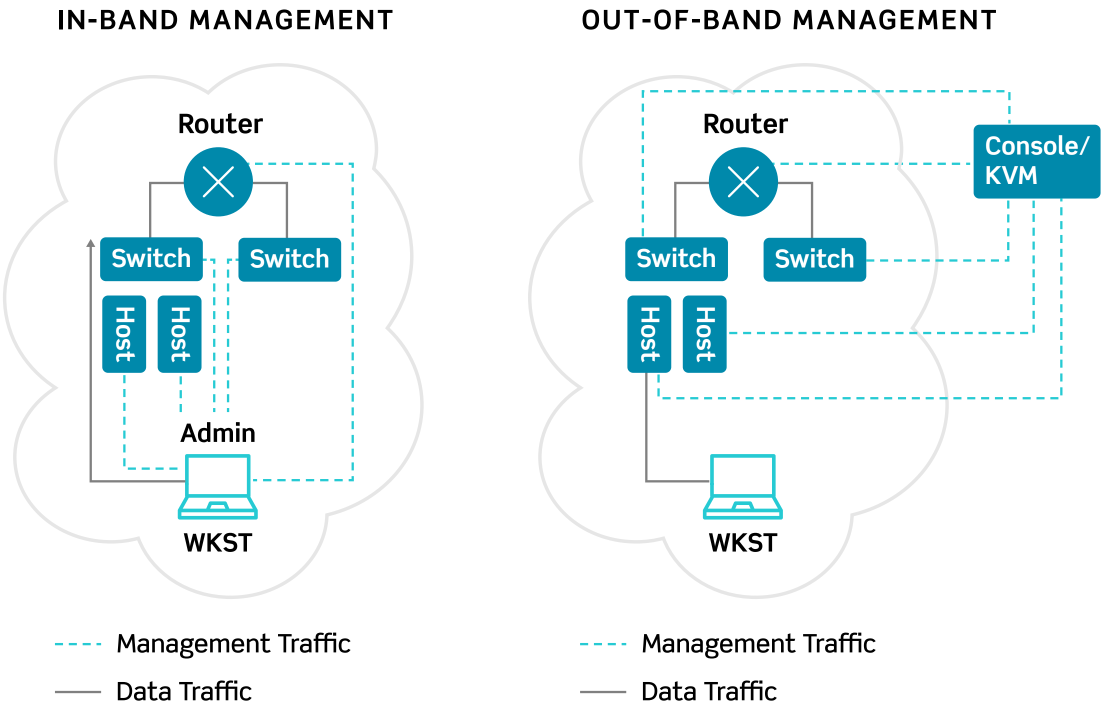

Figure 1: Some of the differences between in-band and out-of-band management

Still, these interfaces rely on a variety of protocols like Intelligent Platform Management Interface (IPMI), SSH, Telnet, Simple Network Management Protocol (SNMP), Serial Console, and Virtual Console.

> Part of the real value that OOBM brings is simplifying device management and administration in a secure manner.

It all sounds overwhelming, right? But the most important feature is that administrators also need to remember a laundry list of commands specific to each device. When you consider that these devices come from a variety of vendors and could be storage, compute, networking, or power devices, keeping track of these commands is no trivial task. But with OOBM, you can greatly simplify management with a single system.

IN-BAND DOWN? OOBM TO THE RESCUE

Another problem that OOBM addresses is the critical requirement for physical access that arises during an outage or situations where there's no network connectivity. Picture this: A network misconfiguration takes down a WAN link 3,000 miles away. The site is entirely offline, and there's no nearby staff. While this sounds like a network administrator's nightmare scenario, it happens.

Without OOBM, it would require a plane ticket and a seven-hour flight for an organization to resolve this network outage. OOBM saves the day by enabling you to quickly reconfigure the switch and restore connectivity via a backup link without ever getting on a plane. OOBM can be made available when the in-band network paths are down by leveraging secondary links like a long-term evolution (LTE) network.

MULTIPLE DEVICE MANAGEMENT

Today, less and less hardware is required to power more applications. Nowhere is this hardware consolidation trend more prevalent than in data centers. The result: outages are impacting a greater number of applications and users.

For this reason OOBM is becoming critical in the next evolution of data centers—managing not only firewalls, switches, routers, servers, and storage controllers—but also supply power like power distribution units (PDUs) and uninterruptible power supplies (UPSes). OOBM is becoming indispensable to keeping network operations running smoothly.

> OOBM addresses the critical requirement for physical access that arises during an outage or situations where there's no network connectivity.

Similar to hardware consolidation, IT teams have seen drastic reductions in the number of personnel. Automation is partly to blame, but so is virtualization that allows any location to serve applications. It's also not uncommon for a remote office/branch office (ROBO) to have no IT people onsite dedicated to keeping the network online. In these situations, should an outage arise, primary administrators must be able to reach the sites remotely to resolve any issues.

TYPICAL OOBM USERS

Now that we've talked about places you can expect to find OOBM, let's explore the organizations that benefit by implementing an OOBM solution.

- **Service providers and large-scale data center** operators deal in a scale of hardware inconceivable to most IT administrators. More devices mean that implementing an OOBM solution can have an even greater payoff when it comes to management ease.
- **Organizations that use colocation facilities** face severe restrictions when it comes to obtaining physical access to the areas that house their hardware. While these restrictions are frustrating during outages, these limitations protect and secure the colocation facility as a whole. OOBM, though, lets you gain physical-like access even in situations where in-band network connectivity is a problem.

- **Organizations where IT isn't physically next to the infrastructure** have IT administrators who are inconvenienced when they cannot walk to the room next door to gain physical access to hardware. Because data centers could be located much further away, OOBM simplifies connectivity and eliminates the need for administrators to waste time traveling to other locations.

- **Organizations with many sites like retail chains, banks, and gas stations** tend to be spread out across a large geographic area. Should these sites go offline, organizations risk losing revenue until an administrator can arrive onsite. Odds are these organizations don't have the staff required to support traveling to these individual sites when time is of the essence. OOBM can eliminate some of the risks posed by prolonged outages operating in a geographically dispersed area.

- **Organizations that must deal with the perpetual pain** of upgrading and keeping in compliance multiple devices spread across the network.

It should be clear by now that OOBM is more than a luxury—it's essentially a requirement for purposes of resiliency and business continuity. Is it worth risking the kind of downtime, and related damage to both profits and reputation you could face when disaster strikes?

To summarize, OOBM is an invaluable tool for your organization. Some benefits include:

- Saying goodbye to the requirement to first gain physical access before troubleshooting. In geographically dispersed areas, OOBM can give you instant access and save your organization hours and days of downtime due to travel.

- Reducing some of the operational burden and complexity that plagues infrastructure teams. These teams must support a variety of interfaces, on an assortment of devices all from different vendors with even more connection methods and commands to remember. OOBM can unify all of this disparity into a single system for management.

- Improving security. Apply another layer of security and implement least privilege when you segregate all device management from in-band network traffic. In addition, OOBM allows you tighten physical access controls in your data center without affecting functionality or your ability to troubleshoot at the console level.

FIND A TRUSTED PARTNER

If it's not worth the risk, the next step is to think about partners that can provide these services for you. One of those potential allies is ZPE Systems, which provides software-defined, vendor-neutral infrastructure management and networking solutions.

> It should be clear by now that OOBM is more than a luxury—it's essentially a requirement for purposes of resiliency and business continuity.

With ZPE Systems, you get control over networking, compute, storage, and smart power assets, regardless of vendor. The company's Nodegrid offerings provide comprehensive and secure remote access and control to your precious systems, keeping you online when it matters most.

When you're ready to take the next step into OOBM, consider ZPE Systems. Check out the company's website, and request a demo today!