ActualTech Media

zpe®

Out-of-Band Networking Design: Best Practices

Ed Tittel

CONTENTS

IN THIS PAPER

Out-of-band management (OOBM) is a critical ingredient in maintaining access to and control over networks, even in the face of network outages or failures. It also helps reduce downtime, avoid vendor lock-in, enhance security, and improve cloud integration.

Out-of-band (OOB) networking refers to the use of communications links that are disparate from those used for production networks. Traditional OOB links use serial connections to dial-up links through a public switched telephone network (PSTN) and its various digital equivalents (ISDN, SIP, and hybrid, hosted, and IP phone systems, and more). However, OOB has evolved. Using modern communications technologies, OOB can also employ cellular wireless connections at up to 5G speeds (1 Gbps and faster). Or they may use wired digital links such as GbE over CATV, Metro or Carrier Ethernet, and so forth.

The central concerns for OOB networks are:

- **Isolation:** OOB networks should have zero overlap with other networks, especially production networks. This applies to interfaces and media used, WAN links and their service providers, and involved networking devices (routers, gateways, and the like).
- **Security:** OOB networks must be impenetrable to anyone except authorized personnel. Ideally, access will require multi-factor authentication (2FA or better), via the most secure links available (VPN or similar protected communications).
- **Accessibility:** Authorized users must be able to access OOB networks even when links go down, power goes out, or disaster strikes. This usually implies multiple points and means of network access, typically with a wired OOB network connection failing over to a wireless 4G or 5G fallback connection when necessary.
- **Availability:** OOB networks must be up and running always, ready for authorized users on demand. Its components and connections must be highly reliable and resilient in the face of outages and failures.

Given that OOB networks meet such concerns, they can provide significant advantages to organizations that put them to work:

- Direct access to equipment—including bare metal unprovisioned devices—allows for installation and setup even when production networks aren't present or are simply not available. This enables network setup and configuration as soon as OOB network elements are in place and working.
- Maintenance and repair—including patches and updates, and system and software recovery or repair—can get underway via the OOB network, independent of production network status or availability.
- Troubleshooting—including diagnostics, break/fix, use of software wizards, and so forth—can get going at any time, independent of production network status or availability.
- Logs and compliance data can be accessed on demand—or when required by some third party such as law enforcement, insurance companies, regulatory agencies, and more—irrespective of production network status or availability.

In short, OOB provides a separate, independent pathway in and out of systems and networks. OOB doesn't depend on production networks to access equipment, perform management and monitoring tasks, make repairs, or access data for legal or technical reasons.

> Good OOB networks result from careful, well-established design and setup considerations and practices.

In the sections that follow, certain well-established best practices for OOB network design and implementation are explored and explained. These should help organizations make the most of their OOB and OOBM capabilities.

OOB Network Setup

Good OOB networks result from careful, well-established design and setup considerations and practices. These may be summed up as two key principles:

1. Make sure the OOB network is completely isolated from production and other networks
2. Test and verify to make sure the OOB network is working (and working properly)

Let's explore these two principles and their implications in more detail.

NETWORK ISOLATION

Network isolation is what makes OOB "out of band." It means that all OOB network interfaces must connect to a network that's separate and disjointed from production networks. In fact, this means separate media and separate infrastructure (switches, routers, WAN links, and so forth) are integral to this isolation, as well. It's best to set IP addresses on OOB networks statically, so they need not depend on DHCP to keep working (and all address assignments should be well-established and well-documented as part of OOB network setup).

Isolation also pertains to access controls. Best practice dictates that OOB networks use access control lists (ACLs) or similar mechanisms (such as role-based access control) to lock down servers, networking components, VPN users, and other elements of the OOB network. Moreover, it's best to use a single, isolated switch or separate router and firewall interfaces for OOBM Ethernet links. Likewise, use a single uplink to a router when Ethernet connections pass through a switch. This not only helps ensure isolation, it also makes it easy to distinguish the OOB network from other networks.

> OOB networks provide a mechanism that's specifically designed for and dedicated to remote access.

One can leave default server accounts intact, but remote access to the server (and other such devices) should be disabled if part of an OOB network. The organization should then set up OOB management accounts with their own well-protected credentials (account, password, 2FA or MFA settings, and so forth). This information should be tightly restricted to authorized administrative and security groups. Best practice dictates that to support auditability and accountability, each authorized user should have unique credentials. In addition, storage and retrieval/access tools for security information must themselves be secured and protected.

Finally, if OOBM features require additional licenses, they should be installed on OOB servers and network components to make them available when and as authorized members of the administrative and security teams need them. This ensures that OOBM can function properly, even if production servers and networks are down or otherwise unavailable.

TEST AND VERIFY OOBM

Once setup is complete, it's absolutely essential to test and verify that OOBM is working properly. Test results should confirm that no access between production and OOB networks and devices is allowed, except for specifically authorized devices (typically, these will be the client devices that admins or security staff use to access all networks).

Further tests should ensure that:

- credentials (secure, proper ACLs or other access mechanisms) are in place and enforced
- the storage and retrieval tools used to manage credentials, configuration data, and other sensitive information is protected from unauthorized access.

Ideally, security testing should include penetration testing that uses technical attacks and social engineering to attempt to compromise or obtain unauthorized access to OOBM systems and networks.

Why Separate Production and Management Networks?

First and foremost, the separation of the OOB network from production networks provides an alternative link to use when production networks go down or link failures prevent remote access to those networks. An OOB network also offers improved security and control for administrative access, thanks to its stringent and tested use of access controls, and secure storage and retrieval tools for sensitive OOBM data.

OOB networks provide a mechanism that's specifically designed for and dedicated to remote access. This lets admins and security personnel get into devices safely and securely, no matter where they're connecting from (HQ, other offices, home, or in the field). OOB networks keep working even when servers or network components fail or won't boot. In fact, they allow admins to perform "bare metal"

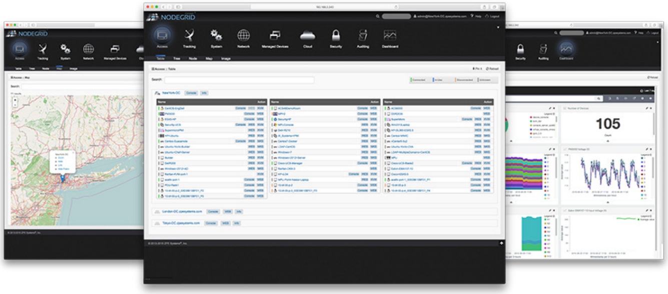

Figure 1: The ZPE Nodegrid Manager provides monitoring and status information for networks and devices, with the ability to drill down, take over, and operate on specific, individual items

installations and configurations remotely even when other means of access, or the networks that provide them, are down. In the same way, OOBM lets admins reconfigure, reboot, or reimage devices remotely across the Internet or via private WAN links.

HOW OOBM TRANSFORMS NETWORK MANAGEMENT

In certain senses, OOBM changes everything when it comes to network management. Thus, for example, instead of dispatching personnel on-site to manually reboot a router, OOBM lets admins do that remotely through an out-of-band connection. If there's some security measure that needs to be enacted (such as blocking some undesirable domain), admins can access the firewall remotely and add a new rule to filter that domain out, thereby blocking access.

OOBM also enables remote troubleshooting. In one case, a communications provider with points of presence (PoPs) around the globe used the serial console to monitor faults and attacks. Thus, it was able to use OOBM to power down switches when a denial of service attack made in-band access and management impossible. Because OOBM means that admins can continue to manage (or disable) equipment even when it's otherwise unreachable, this opens up a bag of remote tricks that keeps organizations in control even when network access problems occur, or attacks get underway.

As shown in **Figure 1**, the ZPE Nodegrid Manager provides tools to access and control both virtual and physical IT devices. This supports installation, setup, troubleshooting, and repair (even bare-metal installations).

Ultimately, OOB stays separate for the best of reasons. It's what provides secure emergency access to servers and other network resources even when production networks may not be working.

HOW TO MANAGE OOBM ELEMENTS: SERIAL LINKS, SERVERS, POWER, AND VMS

OOB management relies on a variety of communications media, usually including serial and/or USB ports. Most OOBM consoles work through RS-232, RJ-11/14/25 and USB 3.0 connections. Some also use 4G LTE or 5G wireless cellular connections, to maintain connections when wired infrastructures become completely unavailable.

In fact, OOBM also works with RJ-45 Ethernet, but such use should be conducted with care and attention. Keeping OOB networks isolated means that RJ-45 Ethernet must use physically disjointed and separate network media and infrastructure. This means separate cables, different IP addresses, different switches (when possible; otherwise, use separate switch ports), and different firewalls and routers (again, when possible; otherwise use separate interfaces within those devices).

OOBM CONSOLE AND MANAGEMENT

For OOBM, a centralized management console consolidates its network and IT infrastructure under a single application view (aka a "single pane of glass"). This is what provides OOB network users with visibility for and access to health and status information. Of course, it's also what ultimately supports remote access to managed devices and networks for configuration, setup, troubleshooting, and repair.

> Managing an OOB network requires extensive knowledge and documentation to match.

The OOBM console works through dedicated management ports that help maintain the rigorous separation between production and OOB networks. For managed/remote devices, this typically means port 1 or 2 will be for remote management access. On the OOBM console, of course, all

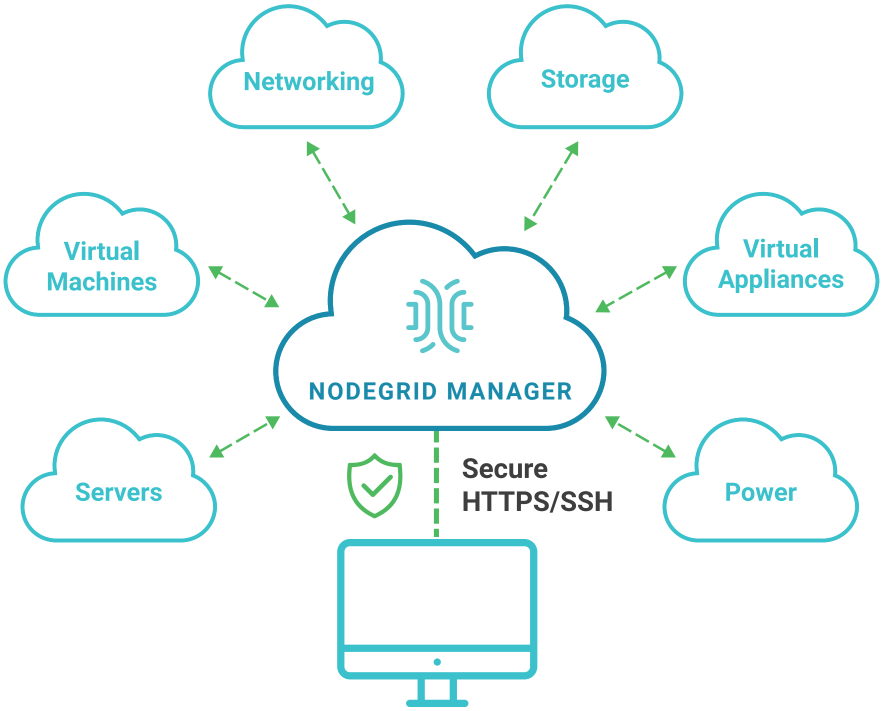

Figure 2: ZPE Nodegrid applications offer ready access to key elements for both OOB and production infrastructure

ports will have OOB access, and there will usually be many of them available, rather than just 2.

Managing an OOB network requires extensive knowledge and documentation to match. Serial and other connection ports must be recorded, along with associated device names, locations, IP addresses, and ACLs properly configured for access and use. ZPE's software eliminates the need to juggle all of this information because it shows the entire network topography.

Servers and other devices should be handled in more or less the same way. Because power (or its lack) can be an issue in establishing and maintaining OOB network access, it's also important to manage power supplies, power connections, and even backup power sources and connections, where applicable. When OOB networks include data center and/or cloud components, keeping track of the same kinds of information—virtual ports, names, IP addresses, access info, and so forth—applies equally to virtual machines (VMs) and software-defined networking (SDN) infrastructure components that belong to an OOB network. **Figure 2** shows ZPE Nodegrid applications, which provide access to power management, VMs, KVM access for remote devices, and more. Each is just one click away from use, whenever admins need them.

Armed with this kind of information, and the ability to access the OOB network, admins and security personnel should be able to cope with whatever fate and fortune may throw their way. The ZPE Nodegrid console device accommodates a wide range of ports, including both Serial and Ethernet, along with 4G LTE or 5G cellular. It also supports connections for additional networking, storage, and compute capability.

Get Started with ZPE

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