ActualTech Media

zpe®

Out-of-Band Management and the Cloud

Ed Tittel

CONTENTS

IN THIS PAPER

OOBM is subject to an ever-widening set of assets and devices, as its scope extends beyond the data center to remote and branch office locations as well. This has taken the basic FCAPS model of network management and extended it into the cloud, while enabling remote access and control via mobile, tablet or desktop client equipment.

This paper discusses how ZPE's product portfolio delivers these capabilities in a way that puts a single, coherent, and consistent console that can handle everything from remote, bare-metal installation or recovery to deployment of virtualized infrastructures and remote or branch office networks. Powerful automation and a consistent, understandable Linux-base runtime and UI leverage existing IT staff skills and knowledge, and provide the tools necessary to create a secure, usable IT environment.

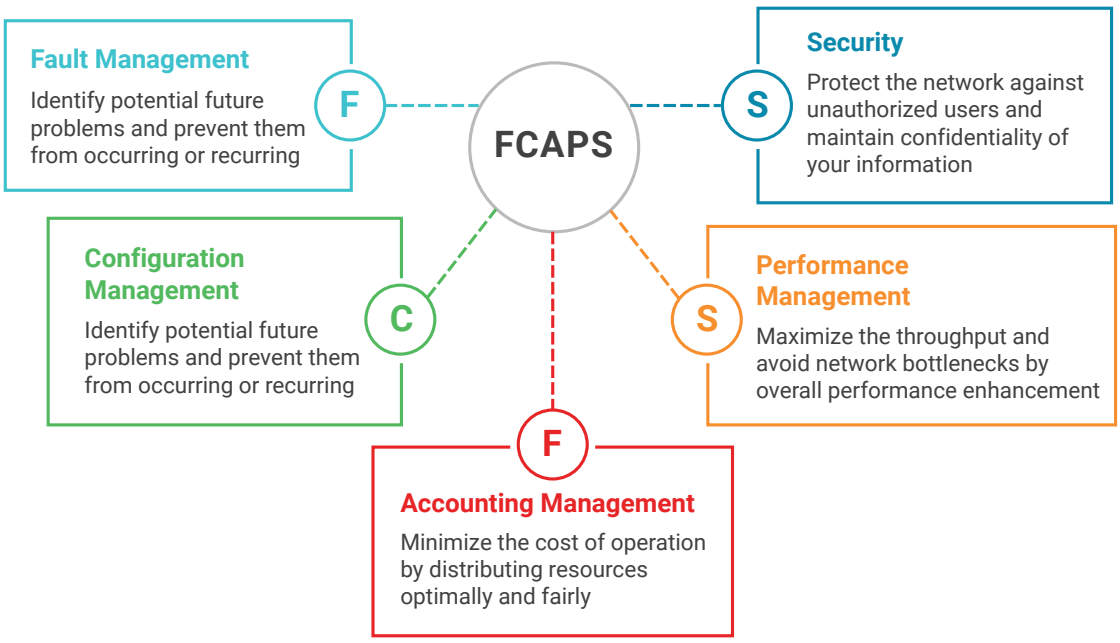

Figure 1: FCAPS was introduced in 1983 as part of the OSI/ISO initiative, and still guides most of what goes into network monitoring and management nearly 40 years later

There's never any question that businesses want to reduce costs, improve data security, and boost DevOps productivity. To that end, organizations can benefit from the right kinds of out-of-band (OOB) IT infrastructure management tools and platforms. Such tools and platforms share a common set of characteristics. They are:

- **Consolidated:** The tools offer a single, coherent, and cohesive view of an organization's IT infrastructure elements and assets through a powerful management console.
- **Smart:** The management software understands how to recognize and organize IT infrastructure elements and assets, along with key health, performance, and security indicators.
- **Vendor-neutral:** The management software works with many and various OSes, platforms, stacks, and frameworks so businesses can keep using what they've got, and can pick and choose best-of-breed elements to bring into their systems and networks.

In fact, ZPE Systems offers a simple, flexible solution for business use. It can replace numerous point solutions, including device- or vendor-specific IT administration tools. ZPE presents a single, simplified, and consolidated portal through which businesses can monitor, manage, and remotely access servers and networking devices using powerful and capable OOB management (OOBM) features.

Basic Principles of Management

Managing systems and networks ultimately means understanding what they comprise, what they can do, and who's allowed to use them. In IT, systems and network management is an important discipline with a long history, with many approaches and tools to implement them.

FCAPS SETS THE MANAGEMENT STAGE

A comprehensive model for network and device management appeared in the 1980s as part of the Open Systems Interconnect (OSI) Systems Management Overview standard (ISO 10040).

This model, shown in **Figure 1**, is called FCAPS, where each letter in that acronym defines one aspect in a network (and device) management framework. FCAPS is best understood as follows:

- **Fault:** Because network faults can be significant, managing them means recognizing, isolating, correcting, and logging them as they occur. Trend analysis of

fault history permits proactive responses to improve network reliability and availability.

- **Configuration:** Configuration represents system set-up and configuration data. Configuration management involves collecting and storing such data, often in a database (usually called CMDB, for configuration management database). This data is tracked, and changes noted and documented. Creating templates and scripts to customize or localize configurations is key to modern provisioning and orchestration.
- **Accounting:** Accounting tracks resources consumed, as well as who uses (or is responsible for) them. Accounting data may be used to generate actual bills, or chargebacks, depending on usage, rates, quotas or allowances, and schedules.
- **Performance:** Performance tools monitor networks and applications for bandwidth, throughput, response time, packet loss and error rates, signal quality, and so on. Performance monitoring may be tied to service-level agreements, availability and reliability metrics, and more. Performance data is key to measuring and monitoring network health. Trend analysis pinpoints capacity and reliability for future planning.
- **Security:** Security management hinges on controlling access to network assets. This includes data security and access security, typically managed using authentication, ACLs, and encryption. Protection against threats is also crucial to security management. It requires a thorough understanding of IT assets in use so related vulnerabilities can be monitored, avoided, or mitigated, as circumstances dictate.

BEYOND FCAPS

As complex and far-ranging as FCAPS is, it represents a somewhat outmoded understanding of what must be managed, and where assets are likely to be housed and situated. It's very much a "pre-cloud" phenomenon in that assets are implicitly and inherently assumed to be owned and controlled by those who use them. Thus, ownership, responsibility, and control were straightforward and unambiguous.

Today, businesses remain responsible for data, applications, and services that run in the cloud. But they share that responsibility with cloud service providers who do indeed own and control the equipment on which these entities run or live. Thus, businesses must understand how FCAPS (and other IT management concerns, such as data protection, reliability and availability, provisioning and orchestration, and cost optimization) plays in the cloud as well as on-premises.

> A proper management console provides ready access to data center servers, networking components, racks, and the power and cooling systems necessary to make them run and keep them running.

This adds both impetus and urgency to the need to aggregate and display alerts, reports, status, and management data under a single, coherent user interface, irrespective of where IT assets, such as computers, other devices, data, applications, or services reside. Such consolidation also permits better visibility into cost and performance data. It also offers better opportunities to manage and optimize such things dynamically, as demand or usage waxes and wanes. This even permits application of consistent, business-driven policies and procedures to IT elements of all kinds, whether on-premises or in the cloud.

Understanding the Management Console

A proper management console provides ready access to data center servers, networking components, racks, and the power and cooling systems necessary to make them run and keep them running. Such a console must also offer simple, powerful automation to carry out repetitive tasks, and support provisioning and orchestration. Ideally, such automation can handle multiple concurrent sessions. Thus, scheduled activities can stay on track,

while automatic responses to alarms, alerts, or threshold conditions occur when triggered.

Likewise, a capable management console must deliver high performance so it can keep up with large- (even web-) scale networks and systems. Thus, support for high baud rates for serial ports (up to 230.4 Kbps) allows for more and faster concurrent OOBM sessions, as does support for USB 3.0 (effective data rates over 1.0 Gbps are widely reported). In addition, high-end OOB devices and consoles may support 4G LTE (effective data rates at 2-5 Mbps) or 5G (1-2 Gbps), so new wireless connections may very well improve OOB network performance.

> Nodegrid gives support staff remote control through a consolidated platform that shows and provides access to everything it can see

Finally, a capable, effective management console should run on Intel x86 CPUs under a 64-bit Linux OS. This lets businesses leverage existing staff knowledge and skills (the vast majority of servers in data centers already run some Linux version). Linux also works well with the best-known scripting languages to better facilitate automation efforts, including Python, JavaScript, Bash, Ruby, Perl, TcL, and many more. In turn, this supports outstanding automation facilities and services from Zero Touch Provisioning (ZTP), to device or server installation and setup, to final configuration, and automated testing and verification. ZPE's offerings—as explained in the following section—meet all of these criteria, and more.

Data Center Management

The historical foundation for IT operations is indisputably the data center. ZPE is expert at providing OOB solutions for data center use, including automation and scripting capabilities, plus flexible ZTP for fast, consistent, and correct deployments. These play well in the hybrid and multi-cloud scenarios prevalent in most businesses nowadays, where data centers are simply elements—albeit important and valuable ones—in a complex, multi-faceted IT environment.

ZPE's data center solutions include the following elements:

- **Nodegrid Manager:** With a powerful "single pane of glass" management console, Nodegrid Manager provides access to and control over virtual and physical IT devices. A software-defined infrastructure (SDI) approach to setup, configuration, and management enables Nodegrid Manager's single-screen console to deliver vendor-neutral control over critical IT infrastructure devices and assets.
- **Nodegrid Services Router and Nodegrid Bold SR:** The Nodegrid Services Router is a modular, open-platform appliance. It provides software-defined networking (SDN), OOBM, DevOps, plus SD-WAN and network function virtualization (NFV), along with support for remote branch offices and retail locations. The Nodegrid Services Router offers optimized and efficient network functions that encompass switching, routing, security, WAN acceleration, secure OOB remote access, and support for Docker or Kubernetes container-based applications. It can also control IT devices at the edge of the network, or within converged infrastructures. Nodegrid Bold SR is a scaled-down version of the Nodegrid Services Router designed for secure access and control over remote and IoT devices at the network edge. Thus, Bold SR also supports NFV and SDN with a focus on SD-WAN capabilities.
- **Nodegrid Serial Console:** A next-generation console server, this device provides secure, hyperscale remote access to all IT devices, regardless of manufacturer.

Together, these elements harmonize to support management of virtual and physical IT devices, including servers and networking, storage, power, and cooling appliances from multiple vendors. Using the ZPE toolset drastically changes the job for support staff. Instead of spending their time, effort, and money on managing a multitude of devices one at a time, Nodegrid gives them remote control through a consolidated platform that shows and provides access to everything it can see.

The ZPE console application, Nodegrid Manager, eliminates the need to access and run point solutions for

typical multi-vendor, multi-provider situations. Instead, Nodegrid Manager delivers common functionality and a common access experience across all devices in the form of an SDI. As new features are added to the console, they're automatically extended to all devices. Thus, administrators can bridge feature gaps among vendors, or even extend native device features, as depicted in **Figure 2**.

Understanding Management Software and Its Touchpoints

ZPE's Nodegrid software drives a thoroughly modern management web portal. Thus, it offers a unified solution for controlling physical and virtual devices and infrastructures. In fact, the console can accommodate Docker- and Kubernetes-based application and service containers. Nodegrid Manager, in turn, can control virtual resources—namely, computer, network, storage, and smart power assets—that such hyperconverged applications and services need to do their jobs and serve their users.

In addition, consolidated IT access and control software saves businesses time, money, and effort. Admins can use the same console, and leverage their UI knowledge and scripting and automation skills, to work with both physical and virtual assets and infrastructures. Even when the environment being managed involves multiple vendors and solutions, the Nodegrid console simplifies efforts through a single, comprehensive, and consistent feature stack across all vendors. This offers explicit cost protection to businesses because they can avoid vendor lock-in, and purchase new hardware and software for their operations purely on price, without having to accept multi-year service contracts, consulting charges, upgrade fees, and the other hidden costs typical of proprietary technologies and platforms.

Built-in SDN support in Nodegrid routers and consoles makes it quick and easy to design and deploy virtualized infrastructures. These can run on commodity hardware, accessed using secure KVMs (generalized

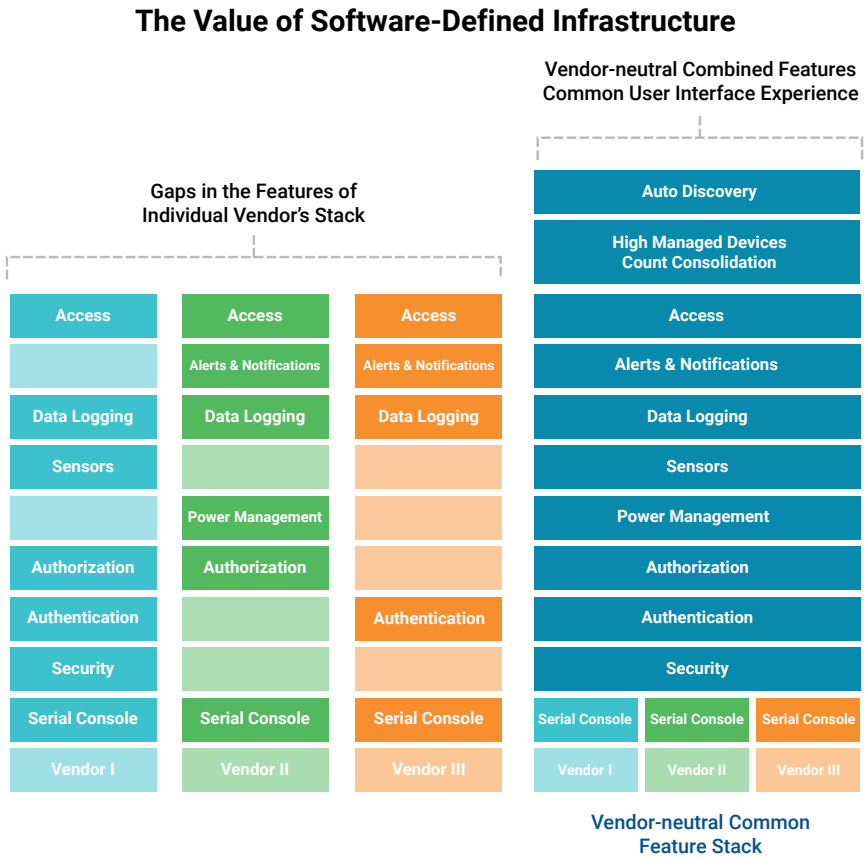

Figure 2: The vendor-neutral console environment consolidates individual vendor solutions under a common UI and feature set, and can even extend or improve upon underlying solution capabilities

keyboard-video-mouse hardware designed to facilitate remote access to computers and many other kinds of networking devices) across secure, encrypted IP and Intelligent Platform Management Interface (IPMI) connections.

Management at (Large) Scale

Nodegrid's OOBM can even handle management for large-scale server farms, with thousands of servers (physical and virtual). At such an operation, a service provider integrated the Nodegrid serial console into its server farm infrastructure. That console served to automate the reboot process for PDUs and IPMI service processors. Consequently, the provider no longer had to send staff on-site to handle that task.

The Linux-based Nodegrid Manager uses policy-based discovery and management tools. That means it can find and identify the assets—including hardware, software, services, subscriptions, and more—on your networks. The same console lets admins and security personnel control, configure, monitor, and manage those assets as well. Better yet, the OOBM tools support bare-metal installs on devices using a bootable ISO (or some equivalent, such as an image or VM snapshot) so that no other software is needed to install or recover your network devices and servers.

> Consolidated IT access and control software saves businesses time, money, and effort.

Overall, Nodegrid Manager and the ZPE devices support fast, simple day-zero provisioning to quickly bring up new devices and network elements. This makes growth and expansion much quicker and simpler, and streamlines and simplifies employee onboarding. This effort typically involves providing a phone or cellphone, a computer, and role-based access to the resources new employees need to get to work. All this can be automated, with simple text files to provide unique one-off information as needed. Thus, Nodegrid relieves IT of having to organize and juggle all these tasks and resources. Everything is automatic, so employees get quick and seamless onboarding.

> Built-in SDN support in Nodegrid routers and consoles makes it quick and easy to design and deploy virtualized infrastructures.

Best of all, Nodegrid Manager and the ZPE devices support flexible remote access. Admins or security personnel can use a mobile phone, a tablet, or desktop devices to get to work. Even remotely, such users have complete support from the command line and through various APIs they may need to access for scripting, automation, orchestration, and so forth. The remote interface also includes web-based search (for help, technical information, and more), books, and additional sources of insight, information, and technical support. **Figure 3** depicts this overall organization of software layers and facilities.

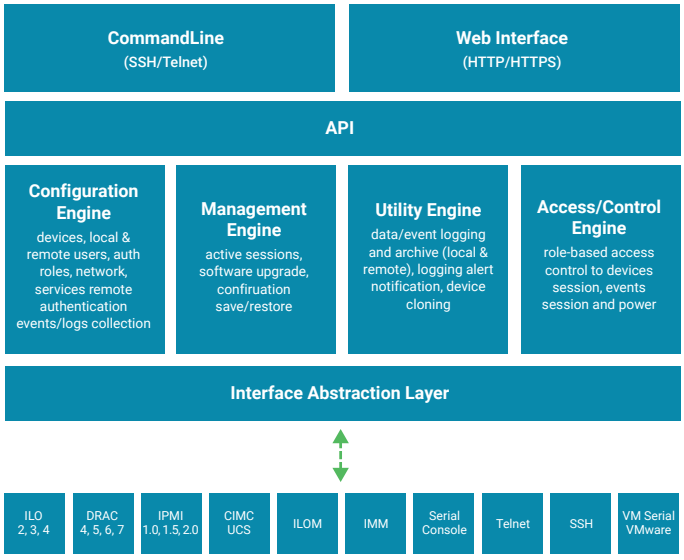

Figure 3: Users accessing Nodegrid Manager (and its console devices) can work through the command-line interface (CLI) or a web-based interface to access the underlying facilities and services it provides

How Is Branch Management Different?

Moving beyond the data center and into remote or branch offices raises a new set of challenges and concerns. ZPE's Nodegrid offers cloud-based IT device provisioning and deployment for branch offices and other remote locations. It includes a simple initial deployment setup to establish a bridgehead from the cloud into the target location. This creates and launches a portal site that provides deployment, provisioning, maintenance, and troubleshooting access to networks and devices at the remote location.

This cloud-based environment offers 360-degree visibility for all network-connected devices. Because of its support for automated installation, setup, and customization, there's no need to ship devices preconfigured. Instead, businesses can save time and money by shipping plain-vanilla or even bare-metal hardware to the remote location. Upon arrival and connection to the network, on-site configuration is quick and easy, with minimal local user input or action required. This provides a boost to security because systems no longer need be shipped with passwords and authentication data pre-installed, which could be sniffed if a malefactor intercepted them in transit. Because they can be shipped without prior customization, there's nothing for the bad guys to find if such systems wind up in the wrong hands.

> Moving beyond the data center and into remote or branch offices raises a new set of challenges and concerns.

Global remote access enables consistent deployment and provisioning anywhere, anytime. ZPE Cloud delivers reliable automated provisioning in remote locations. Behind the scenes, all the data and control come from the security and safety of the network operations center (NOC). Branch devices may be managed over production networks, but OOBM is supported via a wide variety of connections. These include serial, USB, or cellular (4G LTE or 5G, as equipped and available) using IPMI, power management applications, and KVM for access and control.

> Global remote access enables consistent deployment and provisioning anywhere, anytime.

Bonus: All Nodegrid appliances include a Reset Button. First and foremost, this function provides a soft reboot that resets the device to factory defaults. Next, this connects the device on which it's tripped back to ZPE Cloud quickly and easily, with no added hassle for admins or users. It's as close to self-serve repair and restore as modern technology can get.

Call to Action

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