nLogic

opengear
A DIGI COMPANY

WHITE PAPER

Why You Need Out-of-Band Management

System outages can result from cyberattacks, human error, or any number of environmental conditions.

A wide range of network elements can also cause outages. Cable interconnects, power supplies, switches, dense compute chassis, storage arrays, and even air conditioning are potential sources of problems. And network devices are only increasing in complexity, with software stacks that are frequently updated and susceptible to bugs, exploits, and cyberattacks.

ALWAYS-ON ACCESS TO YOUR NETWORK DEVICES

If your primary network becomes unavailable, do all parts of your network, from data centers and branches to edge networks and IoT devices, have connection resilience? As your business grows, your network becomes increasingly complex and new deployments or acquisitions may lack the ability to connect seamlessly through the internet.

Consider these recent examples of major outages and hacks:

- **2015 and again in 2018 – Google:** Theft of private information on Google+ profiles, including name, employer and job title, email address, birth date, age, and relationship status. The breach resulted in Google permanently shutting down the Google+ service.
- **2018 – British Airways:** A hack on the BA website and app allowed the theft of financial and personal data of more than 380,000 customers.
- **2019 – Target:** A two hour outage of the company's registers cost them $50 million in sales.
- **2019 – Facebook:** Multiple network outages, costing Facebook $6.3 million for each hour of downtime. This doesn't factor in the additional losses the company suffered when their stock took a hit.

No business can afford outages, but the bigger your network gets, the more likely they will occur. Outages are costly and may require on site technicians to address at any time. And even firmware updates, configuration changes, and power cycling to correct errors require hands-on help. You need remote access through a secondary connection to give you always-on access to your network devices.

WHAT CAUSES OUTAGES?

System outages can result from cyberattacks, human error, or any number of environmental conditions.

Outages can also be caused by network hardware failures and vulnerabilities in frequently updated software stacks.

One of the most common cause of outages is the vulnerability of the primary network's last mile. While ISP connectivity has improved over the past few years, one weakness these services can't overcome is the last mile problem. This refers to is the final segment of the production network that connects your network to your ISP. This is the weakest link in your connectivity.

In June of 2019, Google Cloud projects running services in multiple US regions experienced elevated packet loss as a result of network congestion for several hours. In analyzing the outage, they reported, "Google engineers were alerted to the failure two minutes after it began, and rapidly engaged the incident management protocols used for the most significant of production incidents. Debugging the problem was significantly hampered by failure of tools competing over use of the now-congested network." They realized they had a problem, ***but they lacked a secondary way to address it.***

All of the network traffic for a single office, store, branch, or distribution center is funneled through single links. The bandwidth of these links effectively limits the amount of data that can be transmitted to your ISP. This bottleneck leaves you exposed to DDoS attacks and basic human error leading to outages. And this last mile can fall victim to physical failure. An accidental fiber cut can knock out your entire network and leave you disconnected from your internet services for significant periods of time.

IN-BAND AND OUT-OF-BAND MANAGEMENT

Your company has a production ISP connection for network traffic including VPN, web, email, cloud apps, and lots more. Often there is only one major network pipe, (T1, cable, SD-WAN, or MPLS), that routes this traffic to the

> *"Being able to get into the equipment that you need; being able to manage, it regardless of whether or not you have connectivity through normal means. So, the 4G, the wireless, all that connectivity is huge."*
>
> **Steve DiCicco**
> *Senior Network Engineer*

internet. Management information flows through the same interfaces as user data. When management and data share this same plane, you end up using the data plane to access your network equipment. This is known as In-Band management. When you manage your equipment using an In-Band network, both data and control commands are traveling across the same network route, so your management plane has the same security vulnerabilities as your data plane. And you may find yourself locked out of the management plane because of the outage.

The advantage of In-Band is that it is cheap and simple since you only need one network. But it is also much less secure because you mix user traffic with typically less strict access rules and management traffic. Outages and attacks could compromise not only the user data but also the management and integrity of your network equipment. Also, when you have an outage, you are unable to communicate with your devices.

Alternatively, you can run the management traffic via a stand-alone network which only handles management traffic. This is Out-of-band Management (OOB). OOB gives you an alternate way to connect to your remote equipment such as routers, switches, and servers through the management plane, without directly accessing the device's production IP address in the data plane and independent of the primary ISP connection your company uses. This Out-of-Band path is completely separate from the production network and allows administrators to securely monitor, access, and manage all devices without interfering with normal operations, and even more importantly, without having to allow data plane level access to the management plane.

Since the Out-of-Band network separates your user and management traffic, you can lock down, restrict access, and thoroughly secure the management plane. Also, you can configure, manage, and troubleshoot your devices even when the data plane is down. An OOB solution offers you a secondary connection, often through 4G LTE, that lets your network technician solve problems from anywhere, and most importantly, saving your company time and money.

The disadvantage is the extra cost of setting up a separate network only for management, but as you'll see later in this paper, the ROI pays for the expense very quickly.

THREE PLANES ARE BETTER THAN ONE

Think of a network as having three planes[1]:

The **Data Plane** consists of the infrastructure components carrying user data". Its purpose is to allow data to flow, for example from a web server to a customer's computer and vice versa.

The **Control Plane** is in charge of keeping data flowing. It contains the rules that allow the routing of information from one place to the other. For example, it enables network routers to come up with a path to take data from a web server to a customer's computer.

The **Management Plane** is used for configuration and management of network switches and routers.

In many configurations, the Management Plane is combined with the Data Plane, which can be problematic when that data plane has issues.

[1] Learn more about network planes.

WHY DO YOU NEED OOB?

Do you really need to add the cost and complexity of a secondary way to connect to your equipment?

Yes, you do. There are several reasons that OOB makes sense, even with an extra cost.

First, you'll have increased security. Without it, the console ports will be connected to your in-band

> *"We were operating our switch stacks and the upgrade failed so we weren't able to get to the stacks any more. Instead of actually driving into the office and connecting through a console port, we were able to connect through Opengear via the cellular module and get it back up and running within 10 minutes. It saved us a lot of time and anguish."*
>
> **Evans Vogas**
> *Network Operations Analyst*

production network, so if a virus, bot, or hacker invades your network, your entire network is at risk.

Secondly, you'll be able to withstand an ISP outage and keep your organization running. Your main internet connection is subject to a "last mile" vulnerability. Something as simple as a backhoe could cut your line and your main connection, whether it's fiber or cable or anything else, is out of commission. And with advanced OOB consoles, managing the outage can be done almost instantaneously, as well as remotely.

For companies with remote offices, Out-of-Band is a no brainer. Instead of having to send a network technician to the site, troubleshooting and administration of your equipment can be done anywhere, anytime, through a centralized management system.

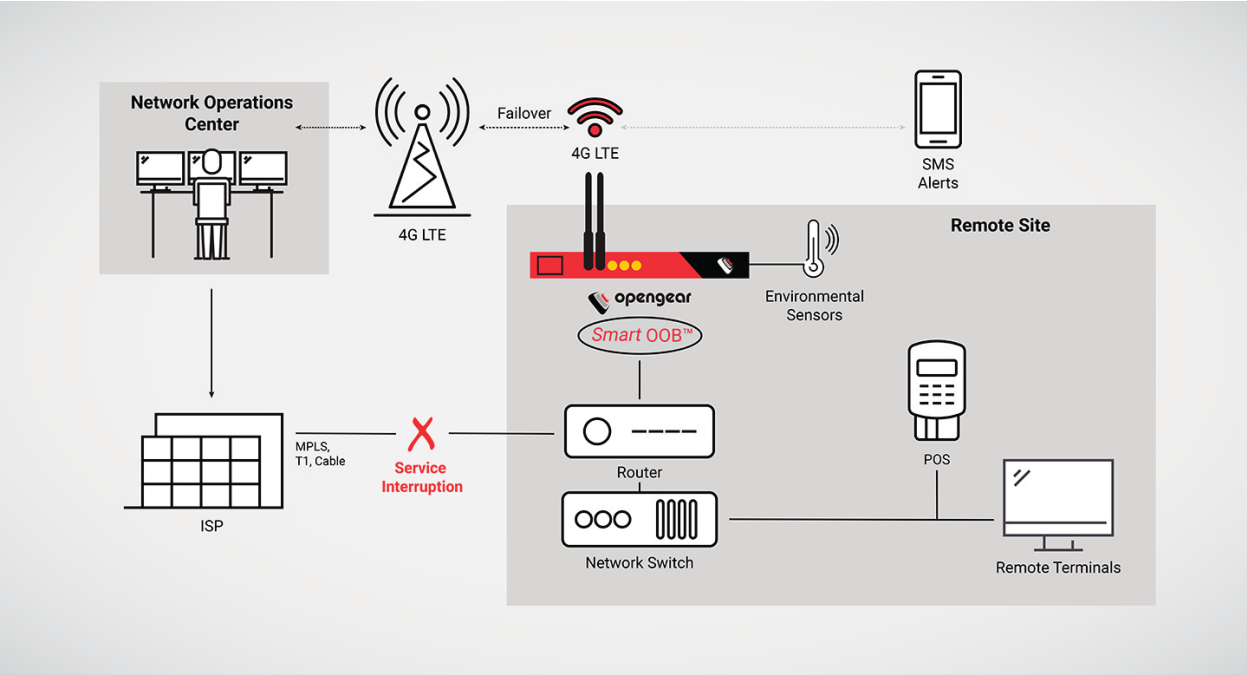
Keep in mind that the LTE bandwidth used to perform administrative tasks is minimal. Basically, network technicians send text commands via a terminal and get information back from those commands. Alternatively, they may be able to use centralized management software that, behind the scenes, still doesn't use excessive bandwidth, keeping the LTE charges low.

Ultimately these advantages will save you a tremendous amount of money, more than making up for the investment in OOB.

TODAY'S ADVANCED OUT-OF-BAND MANAGEMENT CONSOLES

An Out-of-Band management console offers features that substantially minimize downtime and reduce your operating costs:

- Operate independently from the in-band network, which means link diversity for true network resilience.
- Automatically failover to cellular. When the primary link becomes unavailable, internet connectivity is provided for remote LANs and equipment 4G LTE networks.
- Offer Zero Touch Provisioning (ZTP). ZTP lets administrators automate the deployment process. In turn, this allows you to automate repetitive tasks, reduce human touch points, reduce errors, and scale the deployment process to any size.
- Send automated alerts via email or SMS to notify of any network issues
- Identify any inconsistencies or unusual activity with temperature conditions, cage door positions, and network availability.
- Let you remotely get the network back up and running without an onsite visit from a single pane of glass.



"You should be able to come back up without issues after an outage. That's how we design our locations, so that anyone can come in and restart it. Opengear has saved us many, many times."

Landon Orr
Production Network Engineer

RETURN ON YOUR OOB INVESTMENT

OOBconsoles can quickly pay for themselves by reducing operational costs and potentially catastrophic downtime losses. In terms of operational costs, consider the cost of a single edge location going down.

A truck roll could cost $500. An advanced OOBconsole may cost $1500. Just 3 outages have made up the cost. An airplane ride to fix the problem could be even more expensive, reaching a breakeven cost in one incident. And this is just one edge location.

Operating losses are also reduced, since **accordingto Gartner, the average cost of 1 minute of downtime is $5,600**. Consider a network with 10 physical locations.

Now to equip your network with a typical Out-of-Band management deployment with 10 locations and a centralized management system will cost approximately $25k. On average you breakeven after just five minutes of downtime.

CONCLUSION

Out-of-band management eliminates the need for truck rolls and network engineers visiting data centers, branches, kiosks, dispersed offices, or POSretail locations. You can remotely upload configurations and OSimages, simplify backup and restore functions, power cycle routers to reset equipment, and reduce break-fix times. OOBis a huge time and productivity boost for your company. And for your customers, Out-of-Band management can mean the difference between smooth operations and catastrophic failures. If your customers can't access your business, basic trust and loyalty suffer and you get high customer churn.