Opengear's *Smart* Management Fabric (SMF) Technical Brief & Use Cases:

Introduction:

Opengear's Network Resilience Platform helps network professionals to work more efficiently. Our *Smart* Out of Band solution allows customers to deploy, manage, and remediate connected resources from anywhere. Our support for network professionals is constant and comprehensive, on the first day, worst day, every day.

Over the past decade, the networking industry has experienced significant disruptions, such as Software Defined Networking (SDN), the proliferation of open standards, and new technologies like Openconfig and gNMI. To keep up with these changes, Opengear has adapted its out-of-band (OOB) solution for optimal performance.

Traditionally, Opengear's OOB solution offers remote access to network devices and IT infrastructure via serial console and Layer 2 network ports. Our out-of-band network solution has expanded in scope beyond Layer 2 switching. Today, with our new *Smart* Management Fabric (SMF), we are extending our functionality to support our customers by providing seamless Layer 3 connectivity to managed devices and management networks.

Smart Management Fabric (SMF) represents the foundational infrastructure for additional functionality and enhancements that Opengear plans to develop and deliver.

Opengear's Out-of-Band Solution Enables Connectivity

Opengear's out-of-band solution allows users to securely access their network resources remotely, including routers, switches, and firewalls, at data centers and remote edge locations. Typically, when a network engineer, administrator, or IT consultant visits a site to provision, reconfigure, or troubleshoot a problem, they bring along a laptop computer, a serial console cable, and an Ethernet cable. Thanks to Opengear, users have been enjoying continuous connectivity through deployed Opengear appliances for more efficient network operations.

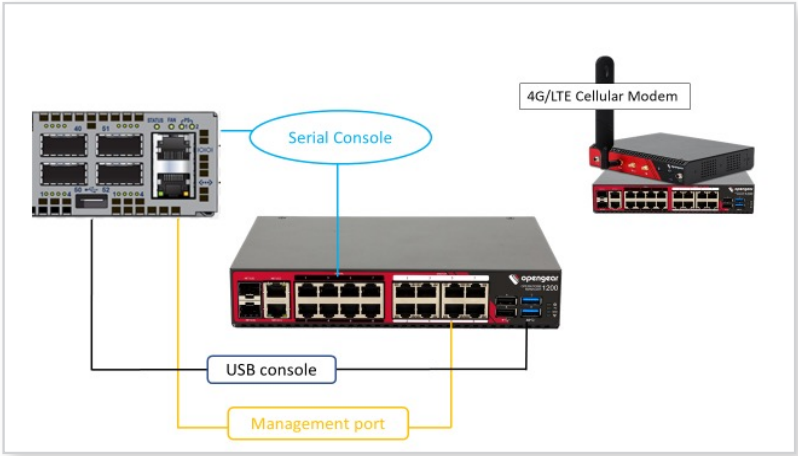

Image 1: Opengear's Out-of-Band Solution Enables Connectivity

A Paradigm Shift in Out-of-Band Networking: Extending Opengear's Network Resilience Platform with IP Access

According to network professionals, the most challenging aspects of their jobs are troubleshooting network issues, remotely setting up devices, managing infrastructure budgets, and designing the network. A crucial component of network design is the management network, which typically does not extend to remote areas of the IT infrastructure. If it is extended, it usually involves only serial connectivity or static IP access.

Opengear's Network Resilience Platform is now more powerful thanks to the addition of *Smart* Management Fabric (SMF), which enables a management network. With the SMF upgrade to Lighthouse Automation Edition (and by using the appliance software version 24.02), users can now easily manage their network with a dynamic routing system. SMF enables network engineers, system admins, and tech support to deploy and access their IP-based connected resources and automation tools easily, securely, and at scale.

Key Benefits of Smart Management Fabric

- **Extended value and functionality of our OOB solution:**

  SMF enhances Opengear's OOB solution to support system admins and tech support teams. These teams can now easily provision and access their server-management tools, such as ILO from HP, IDRAC from Dell, and vCenter from VMware, as well as manage any IP-based physical and virtual resource, such as Virtual Firewall or Virtual Network Function (VNF). Network engineers can use their favorite automation tools, such as Ansible and Python, to provision, monitor, and manage their IP endpoints at scale.

- **Secure streamlined deployments:**

  Config files contain confidential info, like system credentials, logins, and passwords. Giving a third-party engineer local access to such sensitive information when bringing up a new site can be risky. With SMF, users can access and provision their connected resources and keep sensitive info safe. For example, a server-management tool (e.g., Panorama, vCenter, Ansible, FortiManager) can talk to their VMs and appliances through Lighthouse over the OOB network and call Opengear appliances for provisioning, which will keep the info safe.

- **Scalability:**

  SMF is built on widely used, industry-standard technologies. It uses a dynamic IP-routing protocol to enable machine-to-machine and user-to-machine connectivity at scale in an out-of-band network. In other words, by using dynamic routes to facilitate connectivity between the user/machine (i.e., the user's PC) and all network resources connected to enrolled Opengear appliances, Lighthouse learns the network topology and rapidly enables access to these resources automatically within the management network.

Smart Management Fabric Use Cases

Enabling SMF

SMF relies on industry-standard protocols like OSPF routing and creates a secure VPN tunnel to advertise network traffic and routing information. Users can create SMF templates and configure them for their Opengear solution, define their network range and appliance capacity, and easily apply these settings throughout their network. It is available via Lighthouse Automation Edition (link), accessible with Opengear's latest appliance software (NGCS 23.11) in our newest product families, including Operations Manager (OM) 1200 (link) and 2200 (link) and Console Manager (CM) 8100 (link).

Once the users push SMF templates, the system will verify that their devices are SMF enabled/ready and apply SMF templates to their IT environments. Finally, to verify that these changes have been made, users can check the OSPF config files, SSH into their network devices or Opengear appliances to check the CLI of their Lighthouse software solution, then check the CLI of their Opengear appliance. Utilizing these dedicated SMF templates for network configuration brings consistency and efficiency to network management. It helps network professionals dedicate less time to maintaining and managing their networks, and more to priority projects.

1. First day: Simplified Deployment with Smart Management Fabric (SMF)

To enhance efficiency and ensure connectivity for day zero/one tasks, the customer plans to utilize SMF in their management network. First, they aim to set up two-way connectivity and discover all firewalls connected to Opengear appliances; at the same time, they want their firewall to reach their centralized firewall manager. With Lighthouse boosted with SMF, the customer can scan, reach, and provision resources behind Opengear appliances.

The customer utilizes the DHCP server inside the Opengear appliance, where the firewall obtains the IP address and then scans, finds, and registers it to its centralized firewall manager. This essentially creates a management network in their environment.

The customer can now efficiently manage hundreds of firewalls (i.e., Fortinet, Palo Alto) with the help of SMF and a centralized firewall manager (e.g., FortiManager, Panorama). This management network, coupled with an advanced out-of-band feature like SMF and a firewall manager, eliminates the need to log in to firewalls individually to set up security profiles, policies, NAT rules, objects, and routing. With SMF, the customer pushes all of these details and ensures straightforward provisioning and consistency for their management network.

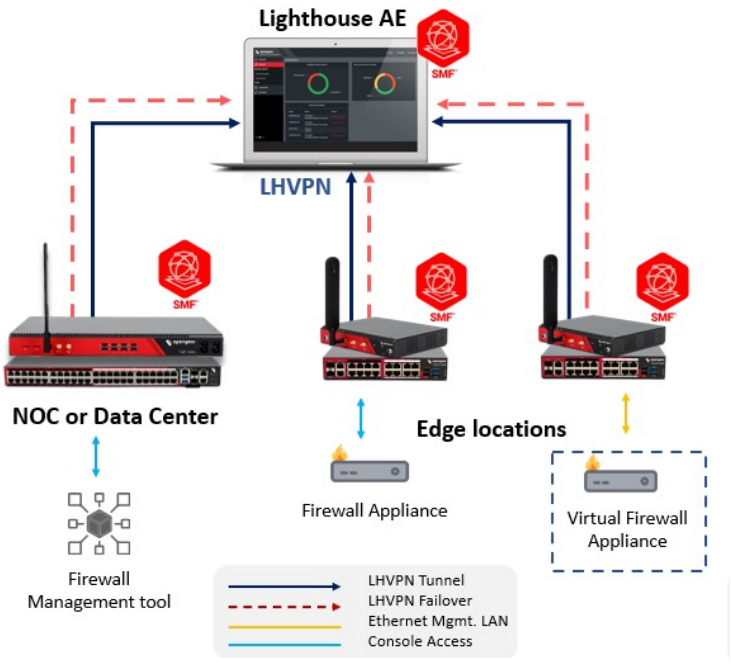

Image 2: First Day-Simplified Deployment with *Smart* Management Fabric (SMF)

2. Worst Day: Troubleshooting with *Smart* Management Fabric (SMF)

When things do not go as planned, customers can rely on Lighthouse boosted with SMF. Serial console connectivity is very useful for network and security engineers, but not all appliances have serial console ports. Over the last decade, we've seen an increasing number of customers begin to deploy virtual appliances, Virtual Machines (VMs), or Virtual Network Functions (VNFs), which lack console ports and are accessed and managed over IP. This is also true of the operating systems and hypervisors that make up an important part of the software stack, the entirety of which must work in order for virtual appliances to operate. Each component in the software stack requires remote access for maintenance and upgrades.

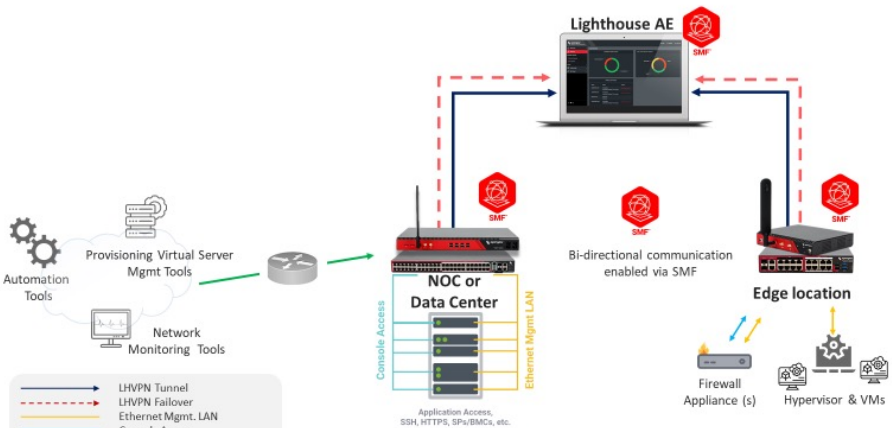

Image 3: Worst Day-Troubleshooting with *Smart* Management Fabric (SMF)

A traditional management network usually does not extend easily to remote locations. When it does, it is often limited to serial connectivity or to the use of static methods to reach IP endpoints. By contrast, with SMF, issues with a network device can be resolved more efficiently.

SMF enables users or machines (e.g., network configuration or automation tools) to reach and remediate any IT resource deployed in any site. Hence, this advanced feature extends the value of the Opengear solution tremendously. It enables dynamic routed IP access, which extends the capability and functionality of our Network Resilience platform.

SMF provides secure remote TCP/IP connectivity to each site in which an Opengear is appliance deployed. In this customer's traditional networking device, the Opengear appliance is providing console access, since SMF is building a proper out-of-band/management network that the network engineers can also access. By taking advantage of SMF, this customer can access VNF easily and remediate any issue that is disrupting the IT environment.

3. Every Day: Monitoring and Managing the Network with *Smart* Management Fabric (SMF)

In this use case, after the customer provisions and configures the Opengear solution, it is ready to serve as the source of truth for monitoring the state of their connected IT/networking resources (e.g., Fortinet, Palo Alto, VMware, Cisco, Juniper, Dell, HP). The customer uses Lighthouse to access, monitor, and manage their network securely and efficiently.

After enabling and configuring SMF as their management network, users can now pass monitoring and telemetry information through the resilient management network to their respective collectors from their networking monitoring tools. The customer is using SMF as a traditional path to make configuration changes to their IP resources rather than performing these changes over their production network.

With SMF enabled, the customer was able to run an automation playbook to ensure their network devices were in compliance (and to upgrade them if needed directly through SMF) and that they were the correct version. Being able to host firmware files securely on every Opengear appliance enabled a faster, more efficient upgrade.

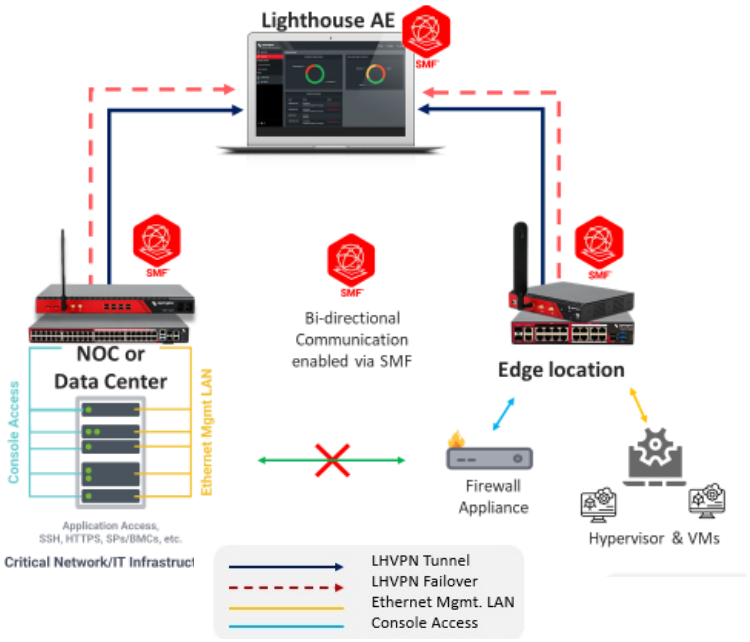

Image 4: Every Day- Monitoring and Managing the Network with *Smart* Management Fabric (SMF)

Which Opengear Appliances Support *Smart* Management Fabric (SMF)?

Opengear's OM1200 and OM2200 Operations Managers and its CM8100 Console Manager support SMF. These appliances also support 802.1Q VLANs and L3 segmentation in the built-in switch ports (on select OM models with this feature), allowing them to connect to multiple management networks or VLANs, as mentioned above. Check out Opengear's network resilience platform demo to learn how it can boost your efficiency.

Summary

The ***Smart*** Management Fabric feature adds a very powerful capability to the Opengear ***Smart*** OOB™ solution, giving customers the ability to deploy, manage, and remediate their IT and network infrastructure remotely with dynamic routing-based IP.

Opengear's network resilience platform helps network professionals to work more efficiently. Our ***Smart*** Out of Band solution allows customers to deploy, manage, and remediate connected resources from anywhere. Check out Opengear's network resilience platform demo to learn how it can boost your efficiency.

Contact Us or Schedule a Demo

If you are interested in the Opengear *Smart* OOB™ solution, have a question, or would like an Lighthouse AE or a SMF feature demo, please contact your local Opengear partner, or contact us directly at the links below:

https://opengear.com/contact-us/

https://opengear.com/schedule-demo/