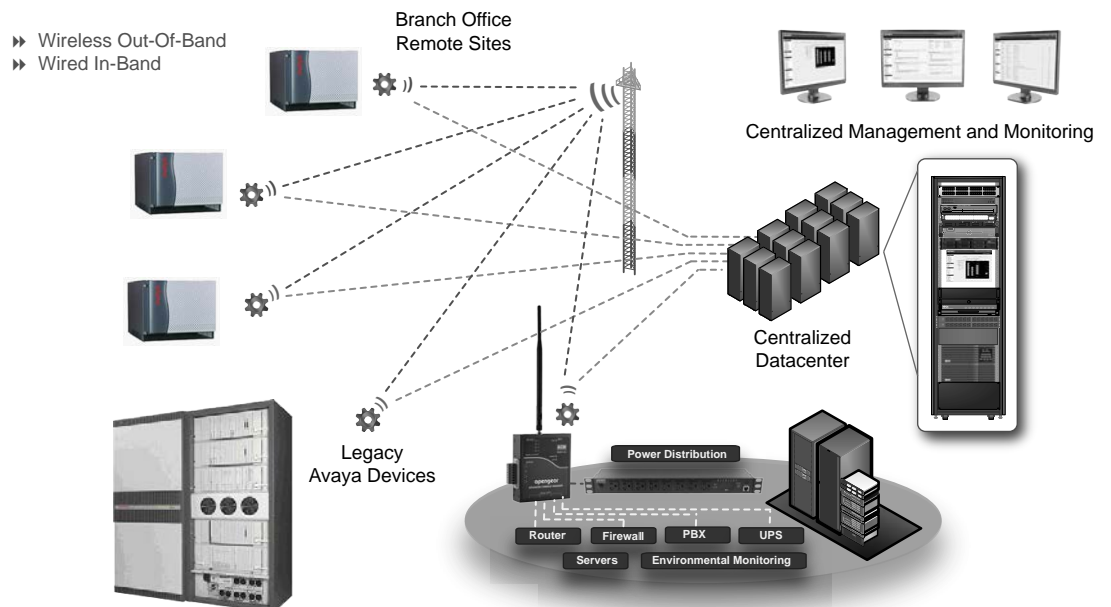




Opengear Technical Note

Jared Mallett - Product Marketing Manager

Opengear solutions deliver cost-effective universal access to Avaya equipment and converged devices installed at customer premise locations. Together, with AlarmTraq monitoring software These unique capabilities have helped Avaya partners greatly improve both the quality and availability of service they provide their customers while reducing overhead costs and eliminating monthly subscription services.



Overview

Avaya is a global leader in enterprise communications systems. The company provides Unified Communications, Contact Centers, Data solutions and related services directly and through its Channel partners to leading businesses and organizations around the world.

Through partnerships, Avaya has teamed up with other leading providers of core switching equipment including Force10 Networks. These convergence of technologies fuse Avaya's market-leading VoIP technology with Force10 high performance switches/routers.

Current Challenges

Customers and Partners of Avaya have been met with challenge to monitor and manage both Avaya equipment and converged devices installed remotely at premise locations. Converged devices are typically core switches and routers to provide the fabric for network connectivity. Many Avaya installations also rely on UPS systems for battery backup during power outages. If any of these components fail the disruption to productivity can be costly.

The current Avaya solution to this problem is the **SAL** Secure Access Link, a hardware and software solution to manage Avaya devices remotely. This is a viable solution, however it does not scale to include connectivity to converged devices, UPS systems or out-of-band access. The Avaya solution requires customers to use corporate internet connections to communicate to the **SAL** Concentrator.

Out-of-band access to distributed IT equipment has been crucial for enterprise customers to eliminate the need for onsite remote IT staff or service calls to handle outages. Not only does this save travel costs, but out-of-band access also reduces recovery time in the event of unplanned outages to ensure remote site productivity. For partners servicing enterprise customers, there is no substitute for secure out-of-band access.

The Avaya **SAL** architecture will require customers to deploy and manage a server for remote access and expensive monthly subscription services to Avaya. This is both costly and limited in function.

Avaya Partners require a reliable remote management solution that would:

- ▶ Minimize on-site service calls in response to service disruptions
 - ▶ Provide a secure, flexible out-of-band solution to ensure uptime
 - ▶ Management and control to all distributed Avaya and converged devices from one centralized location.
 - ▶ Cost effective and scalable alternative to Avaya **SAL**
-

The Opengear Solution

Working closely with Opengear, Avaya partners discovered they could optimize their service offering by deploying a next generation communication management solution that went beyond the offerings of the Avaya **SAL** solution. The Opengear solution allowed partners to scale service offerings to converged devices, battery backup units and secure out-of-band connectivity. The Opengear solution also includes SNMP monitoring and auto-remediation of Avaya systems similar to **SAL**. Having this type of solution in place would help both the IT staff and Avaya partner provide more proactive technical support, reduced on-site visits and enhance management of the communication infrastructure supporting the customer network while simultaneously reducing operational costs.

Components

Opengear - Advanced console servers for remote site management

Opengear console servers monitor distributed IT infrastructure devices including core switching, routers, access points, firewalls, load balancers, servers, and provide a unique ability to automate power reboots and manage UPS systems. We provide IT experts secure access to all devices to perform in-depth diagnostics and troubleshooting within seconds of an incident, and before it affects productivity at the remote site.

Opengear VCMS - Advanced console servers for remote site management

Manage isolated devices that are located behind firewalls, remote console servers initiate outgoing secure SSH tunnels connections to the VCMS. This Call Home feature enables remote control of Avaya equipment and converged devices.

Opengear VCMS provides a single pane of glass to access, authorization and 2 factor RSA SecurID authentication to downstream console servers. Avaya partners and admin users simply point a browser to the VCMS and with a point-n-click they are securely connected to the downstream console server - or managed device - for maintenance, reconfiguration or power cycling.

AlarmTraq - Expert remote alarm monitoring without monthly payments

AlarmTraq™ is the leader in Proactive Remote Alarm Monitoring and Management for AVAYA™ Communications Systems. We go beyond alarm monitoring, we take corrective action. AlarmTraq will not only notify you of alarms it will attempt to remotely diagnose and resolve the problem, even before it becomes service affecting.

These components deliver a flexible alternative to Avaya **SAL** Core Concentrator and SAL Gateways while expanding service offerings to converged devices and enabling out-of-band access for disaster recovery.

Physical Connectivity

There are various ways to connect Avaya devices and converged equipment including RS232 serial, USB, and LAN interfaces. Opengear console servers connect to Avaya equipment using the Maintenance Services Port (LAN) and to legacy Avaya equipment using RS232 serial connections. Enhanced routing and firewall features included with the console server are used to tunnel access to the Maintenance Services Port on the allowed subnet provided by Avaya.

Converged equipment such as Force10 switches utilize RS232 serial console interfaces for remote maintenance and UPS systems using SNMP, RS232 or USB interfaces. Opengear devices can also be ordered with digital I/O interfaces for connecting close contact sensors and triggering warning systems such as a warning strobe light.

Device Connectivity

- ▶ RS232
- ▶ TCP/IP
- ▶ USB
- ▶ Digital I/O

Upstream Network

- ▶ SNMP Alerts
- ▶ SNMP Traps
- ▶ VPN IP Sec
- ▶ SSH / HTTPS

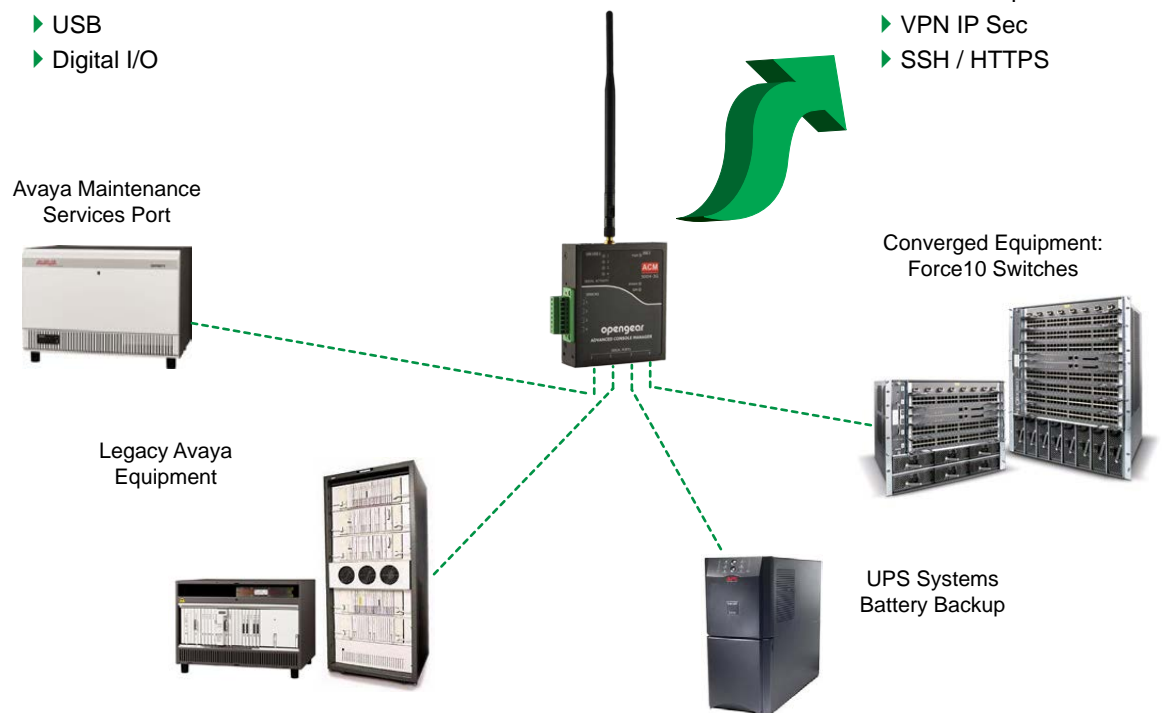


Figure 1.1

Out-Of-Band Connectivity

Traditionally, out-of-band access to remote sites during unplanned network outages has been accomplished using analog modem connections. This solution is secure, robust and still widely deployed throughout the world. As technology changes, the overhead for maintaining analog modem banks at a central location has become an issue for IT management. In addition, most modern laptops lack internal modems to allow for IT staff on the road or working from home to connect easily to remote sites. Opengear has met this challenge with embedded cellular modules that provide high speed data services without wires.

The Opengear solution offers over 100 different products configured with a variety of interfaces to meet any demand. Opengear offers units with internal V.92 modems, redundant LAN, VLAN switch, Wifi and 3G Cellular interfaces. These out-of-band interfaces can be configured as alternate connections during a primary network outage, or the primary source of management from Avaya partners. This solution isolates 3rd party management devices from customer broadband connections when security policy requires physical separation.

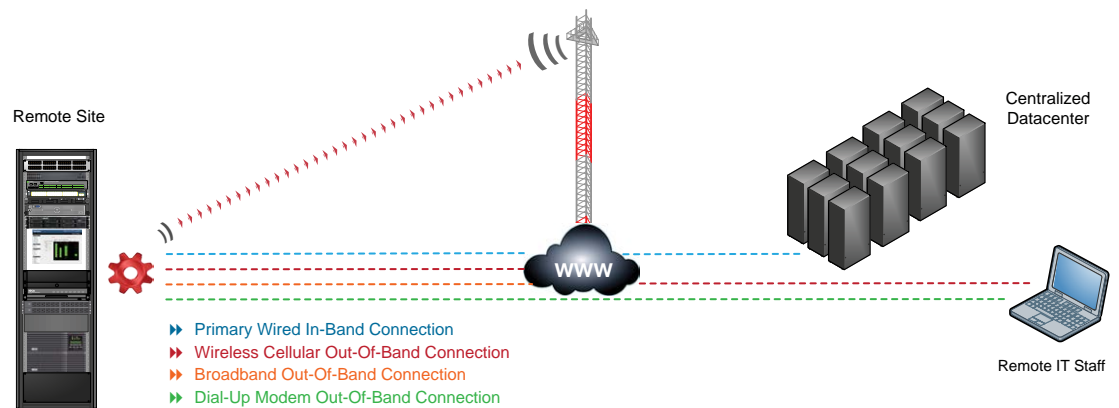


Figure 3.1

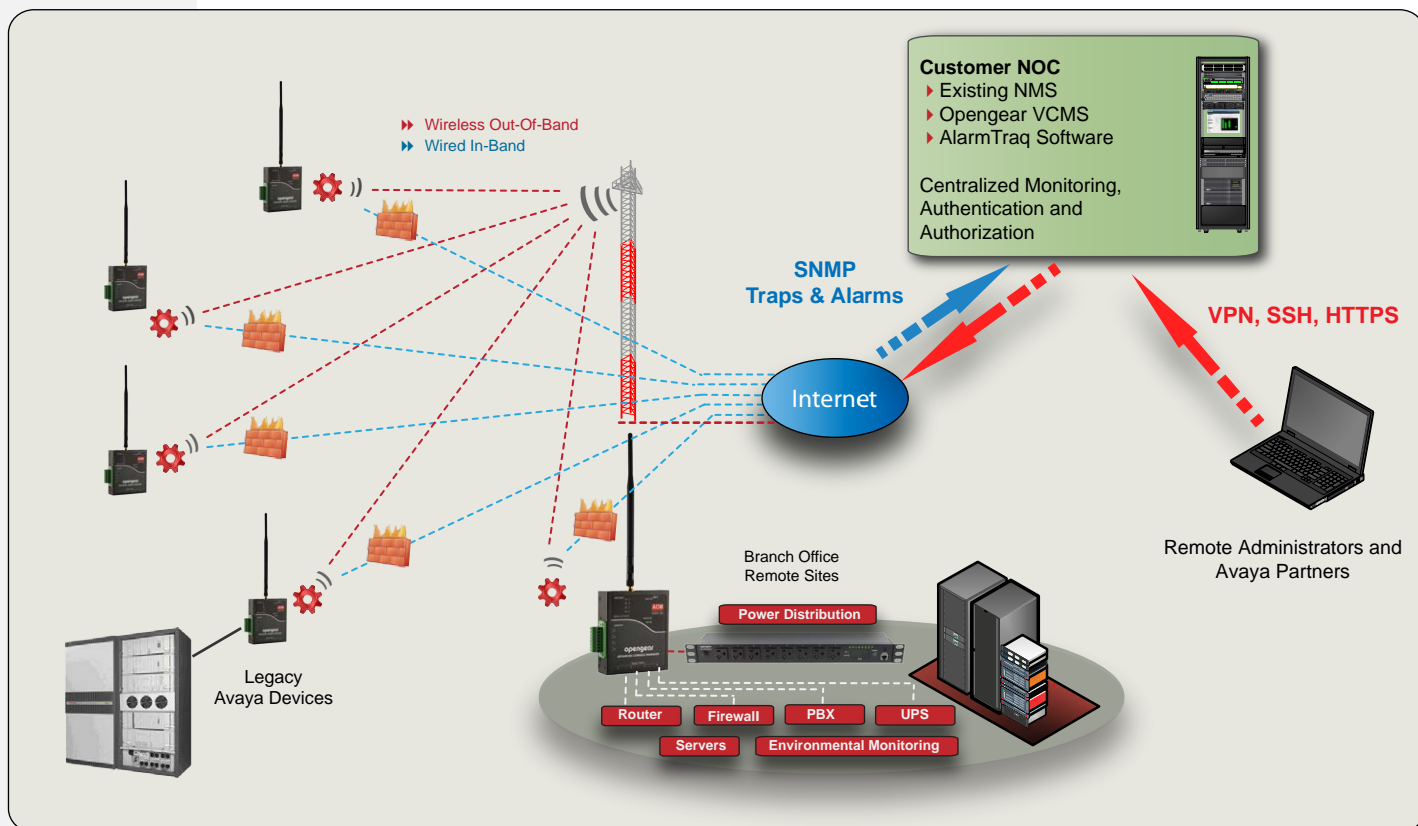
Automatic Failover

The Opengear devices can automatically establish a cellular out-of-band connection, trigger a dial-out modem call or failover to redundant path. The mechanism to trigger a failover connection is activated when both the primary and secondary probe addresses fail to respond. The Opengear devices will automatically connect out bound in a failover scenario and automatically fail back to the primary link once service has been restored.

Secure Centralized Remote Management

Secure two factor authentication through integration with RSA SecurID is a good example of Opengear's support for the industry's most stringent security, encryption and AAA (Authentication, Authorization and Accounting) requirements. To ensure that security and management policies are enforced even during a network outage, Opengear's console server solution:

- ▶ Eliminates common cellular and landline modem security issues with "dial-out" and "call back" connectivity. So if the main network goes down the console server initiates an outgoing call to restore connectivity out-of-band
- ▶ Enables audit and compliance reporting by logging all accesses and changes to the console server and managed devices
- ▶ Supports IPsec, openVPN, SSH and SSL encryption in all devices
- ▶ Maintains and enforces AAA regardless of the state of the network. Under normal circumstances remote TACACS+ or Radius authentication prevails. However if connectivity is lost, the console server falls back to local authentication to maintain authorized access.
- ▶ Provides additional security precautions such as restricting access to specific IP addresses, using encrypted "shadow passwords", providing multiple subscriber accounts and passwords





AlarmTraq and Opengear

AlarmTraq and Opengear have partnered to develop a cost-effective alternative to Avaya **SAL** Concentrator and Gateway solutions. The new integrated AlarmTraq solution uses the Opengear CM4001 and the Opengear ACM5003-M. With this integration, support organizations can securely manage and monitor Avaya Communications Manager servers from a remote location over a dial-up secure SSH tunnel for administration and maintenance.

AlarmTraq goes beyond alarm monitoring, it takes corrective action. AlarmTraq will not only notify you of alarms it will attempt to remotely diagnose and resolve the problem, even before it becomes service affecting. AlarmTraq is sold as a stand-alone server application that runs on your server, so there are no monthly recurring fees for the service.

Why Choose AlarmTraq?

An organization that purchased AlarmTraq back in late 2002 was looking to save money by providing their own remote alarm monitoring for about 100 locations with Avaya Definity systems, with an average size of about 2000 ports (lines and trunks) per location. To support these 100 locations this organization was paying about \$15,800.00/month or \$190,000.00/year for remote alarm monitoring from Avaya. This is based on the typical .60 cents per-port/per month remote-only plan.

They installed a 12-port AlarmTraq server and modems at a cost of about \$12,000.00 one-time, then took advantage of a support plan for AlarmTraq every year since then at an additional cost of \$1,800.00/year. The return on investment was measured in hours instead of months or years. This organization saved over \$930,000.00 the past 5 years because of their decision to go with AlarmTraq.

Who is this organization? The United States Navy.

Conclusion

Together, Opengear and AlarmTraq provide a cost-effective alternative to Avaya **SAL** solutions while simultaneously extending monitoring and management features to converged equipment located in Avaya installs. By leveraging out-of-band capabilities, Avaya partners and customers are always able to manage remote sites even when the main broadband link is down or degraded. These unique capabilities have helped Avaya partners greatly improve both the quality and availability of service they provide their customers while reducing costs.