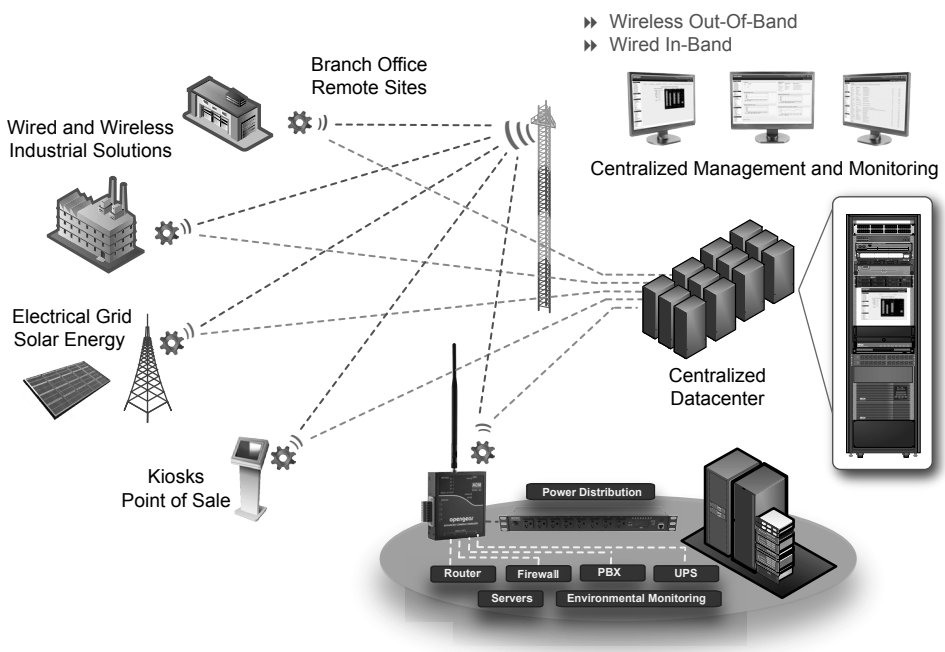
opengear

Cellular Out-Of-Band Access for IT Infrastructure Management

Opengear Application Note

Jared Mallett - Product Marketing Manager

How to Implement Cellular Out-Of-Band Connectivity
to Manage Your Distributed IT Infrastructure using
Opengear Advanced Cellular Routers and Console Servers.



Taming the Complexity of Out-Of-Band Access

Out-of-band access to distributed IT equipment has been crucial for enterprise customers to eliminate the need for onsite remote IT staff 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.

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. The cost of provisioning analog lines at both host and remote locations has increased in part due to the advent of VOIP technologies. This also creates a paradigm where remote sites rely on core switching to provide VOIP analog line access. These same core switches are the gateway for VOIP analog lines which rules out analog modem connectivity during an outage.

The Opengear Solution

We have developed a solution to help control operational costs, eliminate the need for analog modem connectivity and provide a high speed out-of-band access using cellular technologies. The competitive landscape of the cellular marketplace has reduced the cost for cellular data plans to make it even more affordable than using traditional analog lines. Cellular out-of-band connectivity delivers a flexible and secure method for IT staff to connect to remote sites. Opengear cellular enabled devices 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.

This application note outlines how Opengear cellular enabled devices can reduce the cost, complexity and risk of managing remote locations, while also improving the service levels that IT delivers in the process. Specifically, this document will outline the many methods of utilizing Opengear cellular connectivity for secure out-of-band access to distributed IT infrastructure.

Cellular Modem Connection

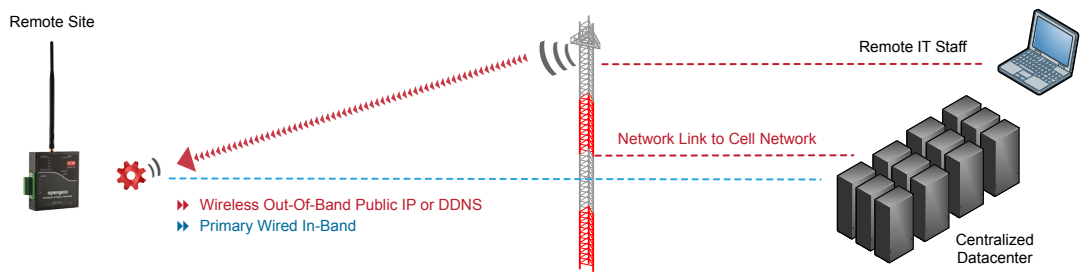
The Opengear ACM5000 and IM4200-X2 families support internal and external cellular modems. These modems will need to be provisioned by the cellular carrier for a data plan. Once provisioned, the Opengear devices can than be configured to operate in variety of modes for cellular connectivity.

In this section we will look at the individual modes available to implementing cellular out-of-band connectivity. Our cellular enabled devices can answer out-of-band connections that are initiated remotely, or they can be configured to initiate the out bound connection from the remote site. Within each available modes available there are some options to include security such as IP Sec VPN and secure SSH tunneling.

To reduce the complexity of public IP addressing our devices are also designed to utilize dynamic dns services and the ability to “call home” to our centralized management platform or SSH server when connected to a cellular carrier network.

Out-Of-Band Connections Initiated Remotely from IT Staff

Call outbound to your remote site over a cellular link



Public IP Address

Opengear cellular devices can listen on the carrier network at both static and dynamic IP addresses. Some carriers offer a premium for a static IP address, while others offer no static IP’s at all. If your carrier provides a static IP address you can simply browse to the Opengear via the web interface and access all connected devices.

Dynamic DNS

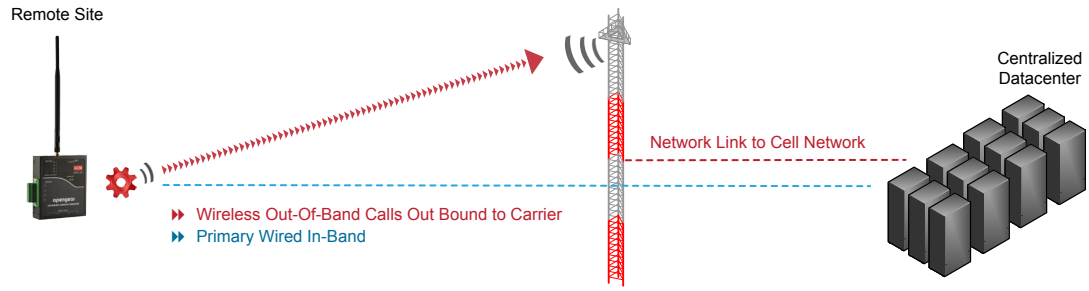
With Dynamic DNS (DDNS) an advanced console server whose IP address is dynamically assigned (and that may change from time to time) can be located using a fixed host or domain name. The ACM500x, IMG4xxx and IM42xx products with Firmware 3.0.2 and later support DDNS. The first step in enabling DDNS is to create an account with the supported DDNS service provider of your choice. Supported DDNS providers include:

- DyNS www.dyns.cx
- dyndns.org www.dyndns.org
- GNUDip gnudip.cheapnet.net
- ODS www.ods.org
- TZO www.tzo.com
- 3322.org (Chinese provider) www.3322.org

Upon registering with the DDNS service provider, you will select a username and password, as well as a hostname that you will use as the DNS name. You can determine the intervals of when the remote cellular device updates the DDNS service with the carrier provided IP address. This allows IT staff to locate cellular connected devices at a consistent address.

Out-Of-Band Connections Initiated from Opengear Device

Automatic failover and recovery initiated by the remote site



Failover Mode

The Opengear cellular connected devices can automatically establish a cellular out-of-band connection to the carrier network when the primary link is experiencing an outage. 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.

Once failover mode has been activated the cellular radio will be enabled, the device will log into the carrier network and then become available to access remotely. At this time you can use Public IP addresses, Dynamic DNS, or establish rules for the device to “call home”.

Call Home

All console servers with Firmware V3.2 and later, include the Call Home feature which initiates the setup of a secure SSH tunnel from the console server to a centralized CMS6100 or VCMS server (referred to herein as CMS- Centralized Monitoring System). The console server then registers as a call home “candidate” on the CMS - and once accepted there it becomes a Managed Console Server. The CMS will then monitor the Managed Console Server, and administrators can access the remote Managed Console Server, through the CMS. This access is available even when the remote console server is behind a third party firewall or has a private non-routable IP addresses, which is often the case when the console server is connected via a cellular modem connection.

Call Home to a generic central SSH server

If you are connecting to a generic SSH server (not a CMS/VCMS) you may configure advanced settings for listening SSH server ports and SSH user to authenticate on the central SSH server. By selecting Listening Server, you may create a Remote port forward from the central SSH server to the remote unit, or a local port forward from this unit to the Server.

3G IPSec connection to a centralized VPN security appliance

The Opengear cellular enabled devices support IPSec VPN’s which can be used to provide a secure connection between the remote site and centralized VPN security appliance. The remote Opengear device can be configured to use this IPSec VPN link while operating in-band and while operating in out-of-band mode the Opengear can rebuild this tunnel over the 3g cellular connection. This feature allows the remote site to retain a consistent address regardless of whether it uses the primary network connection or cellular out-of-band.

Summary

Global out-of-band connectivity that scales to meet any demand

Standardize on cellular solutions to reduce complexity

The Opengear cellular enabled solutions reduce the complexity found in traditional dial-in out-of-band applications where international dialing costs and restrictions prevent ease of access. Opengear solutions are available with temperature monitoring, optional environmental sensors and enables secure management of assets connected via serial console ports, USB, ethernet and digital I/O's. These cellular gateways use the 3G carrier network to deliver real-time access, monitoring and control regardless of location.

High speed wireless connectivity

Opengear solutions can be used as primary wireless network connectivity to assets at remote locations, or can be used as a backup to existing wired landline connections. Equipped with built-in failover capability, these devices automatically switch from a primary wired connections to wireless mobile broadband network during primary service outages and automatically fails back without interruption to service.

Deploy flexible solutions

With several methods of accessing distributed network infrastructure we provide flexible solutions for any scenario:

- *Public IP Address*
- *Dynamic DNS*
- *Automatic Failover*
- *Call Home to CMS/VCMS*
- *Call Home to OpenSSH*
- *IPSec Failover*

IT staff need to be able to connect to and control remote devices even when the network is down. All remote access and network triage need to be done securely, and audited for compliance policies. When the primary in-band network connection is unavailable, a secure, out-of-band path is vital for accessing and managing devices.

Managing distributed IT infrastructure is hard enough. Why make it more complex and expensive by having to buy, deploy and manage multi-vendor proprietary management tools? An integrated out-of-band management solution should be a flexible solution that deploys quickly, begins working immediately, is simple to use and manage, and integrates seamlessly with existing IT management systems.

For more information please visit our website www.opengear.com

USA Head Office
630 West 9560 South
Suite A
Sandy, UT 84070
+1 888 346 6853 (Sales)
+1 801 282 1387 (Support)
+1 801 606 2798 (Fax)
sales@opengear.com

Australian Office
Benson House Suite 44
2 Benson Street
Toowong QLD 4066
+61 7 3871 1800 (Sales & Admin)
+61 7 3720 8289 (Fax)
sales@opengear.com.au

UK Office
Herschel House
58 Herschel Street
Slough, SL1 1PG, UK
+44 776 6866159
sales@opengear.org.uk