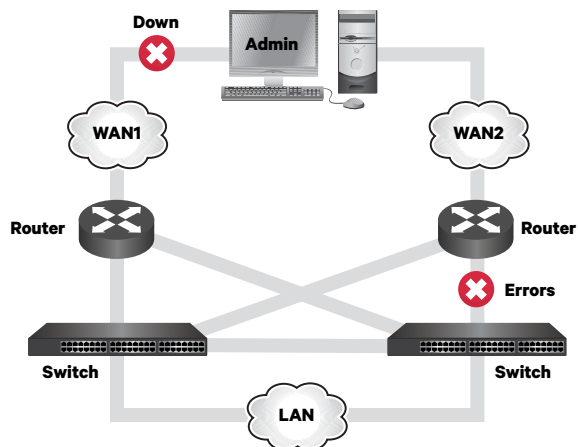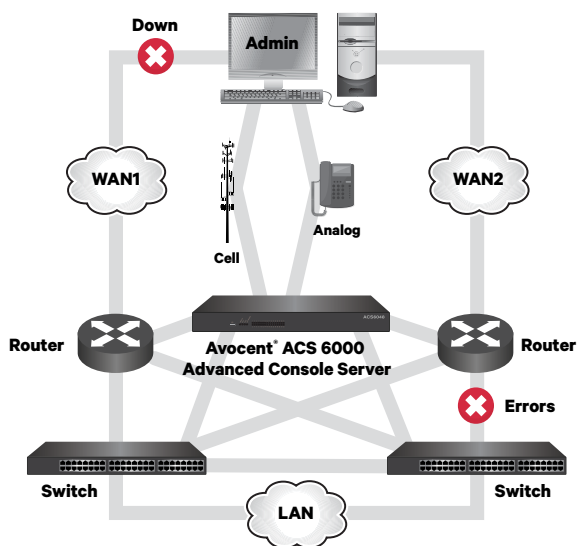# AVOCENT® ACS 6000 ADVANCED CONSOLE SERVER

Remote Access and Control for Enterprise Data Centers

VERTIV

Redundant network without Avocent ACS 6000 Advanced Console Server

Redundant network with Avocent ACS 6000 Advanced Console Server

"Simple issues are dealt with simply, but complicated issues require flexible solutions."

Problem

You've just lost contact with the primary router for the production network on your ERP server farm. Failover was successful and the secondary router has picked up all the traffic, but there's another problem. During a recent equipment move to rebalance the power load, one of the copper switch interconnects on the secondary network was damaged. The network is experiencing significant signal degradation on that link that was undetected until your traffic load failed over to the redundant network. It has effectively cut off fifteen percent of the compute capacity in this cluster. Sales order entry is being impacted and you are losing tens of thousands of dollars every minute that this degradation continues. What's your next step?

The Vertiv™ Solution

With the Avocent® ACS 6000 advanced console server, your administrative staff has the capability to securely access the serial management consoles of you critical infrastructure over the network. In this situation, it allows administrators to remotely connect to the primary router, even though the network interface is down due to a service provider outage. With that information in hand, a quick call to the provider to report the outage is performed without the need to deploy staff on-site to diagnose a dead uplink.

Regarding the damaged network connection, the ACS 6000 allows you to connect both to the upstream switch, which is visible via your management network, but also allows you unhindered access to downstream devices via their serial management interfaces. This damaged copper link can cause enough packet loss to hinder network access to downstream devices. However, your serial links provide the ability to continue diagnosis of the situation from a remote location. This capability allows your administrative staff to isolate the issue to a single link, and deploy a technician directly to the fault location with the correct equipment and tools to perform a quick repair.

The ACS 6000 saves you time and money by providing flexible, reliable, and redundant access to your critical infrastructure. Here are six more reasons that you need the ACS 6000 for out of band access and management of your network infrastructure:

1. Lost network access due to denial of service attacks and/or security vulnerabilities

2. Simple mistakes in the router access list can render the router inaccessible to the network

3. ACS data logging will capture a log of all changes to the router, and who made them

4. The ACS can monitor for, and respond to, port alert messages and state changes

5. Integration with your intelligent PDU allows safe and secure remote power cycling

6. Failed equipment upgrades during security patching can require out-of-band access to recover

AVOCENT® ACS 6000 ADVANCED CONSOLE SERVER

Remote Access and Control for Enterprise Data Centers

The Avocent® ACS 6000 Advanced Console Server

With today's highly redundant, fault-tolerant network architectures, it's often the case that it's the second or third cascade failure that starts impacting your SLAs. Simple issues are dealt with simply, but complicated issues require flexible solutions. With the Avocent ACS 6000, you have several opportunities for intervention that can be faster than dispatching a technician - especially for remote, lights-out data centers, or locations where you have to drop time-critical tasks to make multiple trips across large data centers to diagnose, then dispatch and deploy, replacement equipment.

The ACS 6000 allows secured network access to serial consoles and infrastructure equipment. Examples of typical equipment that can be serially managed are network routers and switches, wireless access points, firewalls and security appliances, intelligent power distribution units, uninterruptible power supplies, storage arrays, blade server chassis, telecom equipment, and myriad other devices. While many of these devices can be managed over their network connections, or even over out of band management network ports, the serial console often allows simplified and more complete control over the administrative functions of the device. Having an ACS 6000 attached to your infrastructure serial management ports means never having to explain why technical support staff could not access the malfunctioning network switch because their tablet or laptop only had USB ports and could not attach to the RS-232 management port.

The ACS 6000 secures these administrative serial ports with industry standard encryption implemented with an embedded FIPS 140-2 validated encryption module. This module implements the requirements of the US Federal Information Processing Standards; a set of standards developed by the US government for securing data housed in government systems. The ACS 6000 also ensures the safety and security of critical infrastructure by providing centralized authentication, authorization, and accounting. Remote connections to devices can be SSL encrypted and access to devices can be managed standalone, or integrated with your existing Radius, TACACS+, Active Directory, LDAP, or Kerberos infrastructure.

Local and remote logging support ensures that any and all access to target devices can be monitored and reported. Local logging can be performed to the onboard storage of the ACS 6000 or to removable storage media. This flexibility in storage options enables organizations to implement records retention policies in several ways - and enforce it through manual rotation and erasure of storage media.

Redundant Network Access

Dual Ethernet ports on the ACS 6000 provide direct access capabilities to serial devices from a redundant, out of band management network. In the example above, even though a service interruption rendered the primary network interface inaccessible, critical infrastructure was still accessible using the secondary network interface of the ACS 6000. This redundant access allows administrative staff to access devices, diagnose problems, and potentially implement mitigations or corrective actions without deploying people and equipment onsite.

"While many of these devices can be managed over their network connections, or even over out of band management network ports, the serial console often allows simplified and more complete control over the administrative functions of the device. "
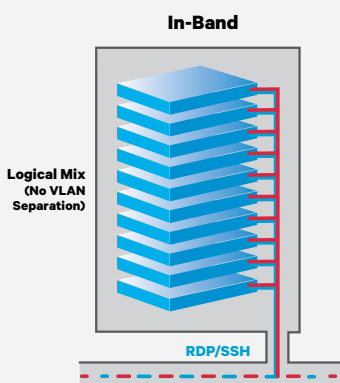
The ACS 6000 also supports access to managed devices via an optional analog modem port. These days, analog modems are often thought of as obsolete, but as is often the case, older, proven technologies can be more robust and reliable than newer options. When the network goes down, or an accidental misconfiguration renders it inaccessible, the ability to fall back to a simple, dedicated modem line can be the difference between remotely recovering from the outage and deploying support staff. This becomes even more beneficial when considering remote and branch office locations that can be days from support centers, or when managing equipment that is deployed in industrial or hazardous locations that are difficult to reach, or which can only be reached safely by bringing down important production equipment.
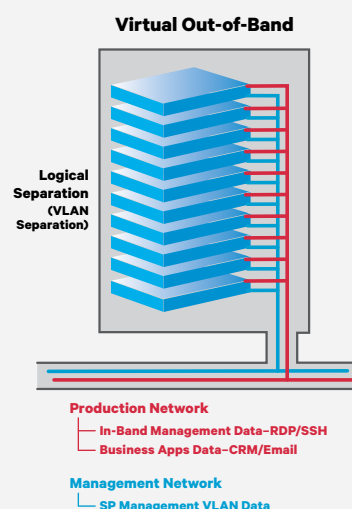
Remote access and control the Vertiv™ way

There are many reasons for implementing a remote management system, from improving safety to increasing productivity. No matter the end purpose, planning should start with careful consideration of the network. There are three common approaches to creating management networks:
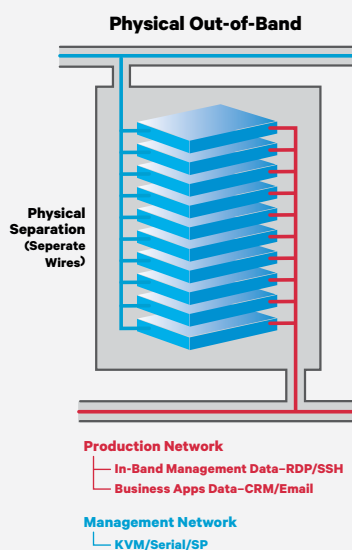
- In-Band - Using the production network to access management ports

- Virtual Out-of-Band - Using a management VLAN on the production network switches

- Physical Out-of-Band - Using a dedicated management switch and cabling

Virtual Out-of-Band

Logical Separation (VLAN Separation)

Production Network
— In-Band Management Data–RDP/SSH
— Business Apps Data–CRM/Email

Management Network
— SP Management VLAN Data

Virtual Out-of-band networks are a step up from In-band networks, but still have the problem of sharing physical cabling. Any issues with interconnection will affect the management as well as the production traffic, rendering the management network ineffective in diagnosing and resolving issues. Then again, for attackers sophisticated enough to gain access to your production network, it's a simple thing to migrate to the management network when cabling is shared.

In-Band

Logical Mix (No VLAN Separation)

RDP/SSH

In-band management networks tend to be the first deployed because they are the simplest to implement. Nothing needs to be done except plug in devices. However, with the growing threat of security vulnerabilities – both within and outside the enterprise – attaching powerful management interfaces to the production network is no longer advised.

Physical Out-of-Band

Physical Separation (Seperate Wires)

Production Network
— In-Band Management Data–RDP/SSH
— Business Apps Data–CRM/Email

Management Network
— KVM/Serial/SP

Physical out-of-band networks are the preferred implementation. Dedicated wiring, switches, and management interfaces are used to separate the administrative functions of your infrastructure from the production network. Not only is this more secure, but it provides true redundancy of access and control for when outages occur. This need not be an unnecessary expense for the enterprise - often times, equipment that has aged out of usefulness for production traffic can be repurposed to deploy the dedicated management network.

For those locations where installation of an analog modem line is not available, or simply not cost effective, the ACS 6000 supports several optional 3G, 4G, and LTE cellular modems. These devices have the same remote benefits as an analog modem line, but the benefit of accessing the modern cellular network which has reached many parts of the world where copper deployment is not feasible. It is also a benefit in data centers where equipment may be redeployed often to handle the changing needs of the business. In this case, running Ethernet cables to each rack is required, but analog modem lines may be a luxury. Cellular modem access can give you that additional layer of redundancy you need, while allowing the flexibility to deploy anywhere with a cellular signal.

Summary

The Avocent® ACS 6000 provides secure, out of band, management of your serially managed devices. It provides a simple solution for aggregation of serial management consoles via a hardware appliance that provides a single solution for authentication, authorization, and accounting of access to your critical infrastructure devices. The redundant network capabilities in the ACS 6000 – dual Ethernet ports and optional analog and cellular modems – provide the flexibility that organizations need to deal with complex systems outages in a way that saves money by allowing more instances where remote diagnosis and mitigation can be employed.

For more information, contact your local sales representative or visit our website at **www.VertivCo.com.**

AV-43108 (R07-15)