

IMPROVING BUSINESS CONTINUITY FOR THE REMOTE OFFICE



EXECUTIVE SUMMARY

Remote System availability is critical to maintaining business continuity. Network outages and related disruptions in services account for significant losses in both productivity and revenue. Traditionally, organizations have built redundant infrastructures at remote sites to ensure the stability of the network. Companies today are considering whether they can cost-justify complete infrastructure redundancy across multiple sites for the sake of improved business continuity.

Driven by the advent of IP-based remote management technologies, businesses with remote offices have turned increasingly to cost-efficient centralized IT management solutions. These solutions, while impressive, are not without associated risks. IP-based access solutions (also called “in-band” solutions”) are dependent on the Internet for remote access to the infrastructure. An alternative path, or “out-of-band” access, to devices within the IT infrastructure is necessary if Internet-access becomes unavailable for any reason. Avocent offers a comprehensive suite of tools that leverage out-of-band technology to enable access to business critical hardware, even in the absence of network connectivity.

THE COSTS OF IMPAIRED BUSINESS CONTINUITY IN THE REMOTE OFFICE

Businesses today rely on, and expect, 24/7 system availability. And while system availability is just one of the many factors contributing to business continuity, it is among the most critical. Given the increasingly IT-centric business landscape, a lapse in system availability can result in severe ramifications, including the following:

- **Lost productivity.** In its simplest form, lost productivity is the product of the number of a worker's productive hours lost to an outage and the worker's salary per hour. More sophisticated calculations measure the financial impact of lost productivity (e.g., lost profit from the work that would have been produced during the outage), or subtract the relative value of alternate work performed during the outage from the base calculation.
- **Additional labor cost.** These include outsourced IT, overtime for all affected staff, transportation of IT workers to the remote site or transportation of remote workers to an alternate location, and the cost to other projects of IT staff reassignment during the outage.
- **Short-term business loss.** This includes any sales or service revenue lost at the remote office during the downtime.
- **Long-term business loss.** This is an estimate of customer abandonment costs that might occur as a result of downtime. This cost is industry-specific and business-specific, so IT managers should examine previous outages within their business or sector for estimates, if possible. Long-term business losses are particularly important to commodity businesses without physical goods, such as financial services.
- **Remediation costs.** This includes any fines, judgments, and legal fees incurred as a result of an outage, such as Service Level Agreement (SLA) breaches, privacy policy violations, and regulatory non-compliance. Remediation costs also include any crisis management costs and advertising aimed at restoring consumer or partner confidence.

Branch Office Downtime & Degradation Costs are Significant

Industry	Avg # Branches	Downtime Hours/Yr.	Degradation Hours/Yr.	Avg Lost Revenue	Avg Lost Productivity
Finance	212	719	461	\$56 M	\$165 M
Health	62	180	213	\$17 M	\$25 M
Trans	101	172	126	\$14 M	\$18 M
Mfg	159	393	373	\$80 M	\$74 M
Retail	174	322	196	\$18 M	\$23 M

COMMON METHODS FOR IMPROVING BUSINESS CONTINUITY

Traditionally, remote offices have improved the resiliency of their networks through hardware redundancy and in-band management solutions.

Hardware redundancy

One of the simplest ways to protect against hardware failure is to locate backups for critical hardware on-site. For certain classes of hardware, most notably hard drives, this strategy works well. Hard drives are inexpensive, and mature standards such as RAID automate backup drive maintenance and failover.

For other, more complex, more expensive classes of hardware, hardware redundancy may be impractical. In the absence of RAID controllers or their equivalent, maintaining mirrored hardware configurations requires administrators to configure multiple devices with identical settings, patches, and add-ons. This overhead is difficult to justify in a remote office that is already short on IT staff.

Hardware cannot replace the need for human staff. Even a complete, on-site backup requires an IT staff member to exchange parts, and duplicate hardware cannot help the central office diagnose problems stemming from application configuration or connectivity. Most large enterprises upgrade their support contracts to provide fast replacement of expensive, critical hardware, but even these contracts require on-site IT staff to diagnose the problem before the vendor will dispatch a replacement.

In-band management

IT administrators typically monitor the remote office infrastructure using IP-based management solutions. This software assumes various forms, including virtual terminal servers, telnet sessions, or browser-based consoles. Some server vendors offer embedded management hardware cards in their systems that provide detailed environment information and device-level configuration options to a custom console.

The IP-based systems are referred to as “in-band” because they require a proper-functioning network (typically an IP-based network such as the Internet or a WAN). If the network connection between the administrator and a remote device fails (i.e., becomes “out-of-band”), the application is useless until the network connection is restored.

OUT-OF-BAND MANAGEMENT

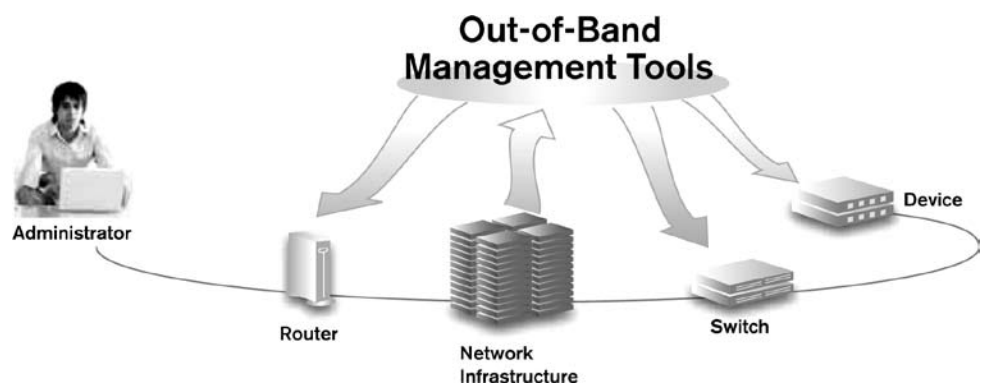
From a business continuity standpoint, in-band management systems pose a significant problem—they fail at exactly the time when they are most needed. If network access is unavailable due to a service outage, router malfunction, or other disruption in

service, in-band access will not work. To address this, technology providers have created a new class of “out-of-band” management tools. Unlike strictly IP-based in-band solutions, out-of-band tools provide a secondary path to the remote site for use when the primary network is impaired.

Consider the following example. The network connection to a remote office has failed, and remote employees are unable to work until it is restored. Network administrators cannot use any of their in-band tools to assess or remedy the situation. With no visibility into the remote location and little idea of the cause of the problem, the administrators are forced to send in-house staff to their site, hire expensive contractors to diagnose the problem, or rely on phone-based walkthroughs with non-IT remote staff.

Out-of-band technology significantly alters this scenario, allowing network administrators to dial into a remote Keyboard-Video-Mouse (KVM) or serial switch, viewing the screens of any non-responsive devices and diagnosing the problems. With remote power management in place, administrators can even perform hard restarts of systems, often restoring full functionality without ever leaving the central office. If the problems require on-site staff, the central office can dispatch the *correct* staff for the issue at hand, based on remote diagnosis, saving money and time, and returning remote workers to their jobs faster.

Out-of-band management typically requires a serial console server at the remote site. When connected to the remote site’s IT assets (e.g., routers, switches, and other devices), the serial console can be securely accessed via a dial-up connection over the PSTN (see Figure 1). In other words, if the ISP is experiencing a network outage, the remote location can still be accessed via a dial-in connection. Secure out-of-band access via dial-up to a serial console server ensures that networked devices are always accessible, even when connectivity is lost.



Even with the network down, administrators can access out-of-band management solutions through an alternate path, such as dial-in.

Complementary to remote management solutions, out-of-band access functionality offers more robust access to IT infrastructure assets. Operational costs are reduced and the need for hardware redundancy is minimized.

IMPROVING BUSINESS CONTINUITY WITH AVOCENT

OUT-OF-BAND SOLUTIONS

Out-of-band management products provide centralized control and repair of local and remote IT infrastructure, even when connectivity is lost or devices are down. Avocent® is the leading vendor in this space, providing businesses with a single interface to quickly and efficiently manage their remote infrastructures. Related products include the Avocent Cyclades® serial console servers, the Avocent DSR® line of KVM over IP switches, and Avocent DSView® 5 management software. Together, this suite of products provides comprehensive out-of-band, remote IT management.

Cyclades Serial ACS console server

The Cyclades ACS family of advanced console servers enables IT administrators to perform out-of-band management of IT assets from anywhere in the world. The Cyclades ACS console server provides enterprise and telecom networks with a complete, secure console management solution. When combined with integrated power management and centralized administration, the Cyclades ACS console server offers a secure and consolidated out-of-band infrastructure management solution. Using a hardened Linux operating system, the Cyclades ACS console server provides optimal performance, security, and reliability. The serial console port is the only platform-independent, out-of-band access appliance that will connect to all equipment in a remote office location. When used in conjunction with complementary management solutions from Avocent, business continuity is significantly improved.

DSR KVM Switches

DSR KVM over IP switches provide BIOS-level control of all connected servers and serial-based devices in the data center. DSR switches allow administrators to remotely manage and power cycle connected devices. The DSR switch enables out-of-band access via a port that can be connected to a modem. This provides access to the switch when the IP connection is not functioning. Avocent DSR KVM switches feature an on-board Web interface compatible with Internet Explorer, Mozilla, Firefox, or Netscape browsers for access and control of servers over IP. IT administrators can use DSR KVM switches to manage remote data centers and branches as if present in each location. This reduces downtime by providing easy access and control to any connected server or device.

DSView 3 Management Software

Avocent DSView 3 management software is a single, secure interface that allows administrators to tame complexity, manage growth, and keep critical systems healthy and available. DSView 3 software enables secure, centralized management of all connected IT and network devices in today's often complex and geographically dispersed data centers. When used in conjunction with out-of-band hardware solutions, DSView 3 software allows IT administrators to remotely access, monitor, and control target devices on multiple platforms at numerous locations via in-band or out-of-band access.

ABOUT AVOCENT

Avocent is a leading global provider of IT infrastructure management solutions for enterprise data centers, small/medium businesses, and remote offices. Avocent's unique integration of hardware, software, and embedded technologies provides a single interface to quickly and efficiently manage IT infrastructures. Avocent help its customers solve system problems anytime, anywhere, regardless of the location or health of the servers or network devices.

For More Information:

AVOCENT CORPORATION

4991 Corporate Dr., Huntsville, AL 35805

TEL: 256-430-4000

FAX: 256-430-4030

TOLL FREE: 1-866-286-2368

www.avocent.com



Avocent[®]
The Power of Being There[®]

Corporate Headquarters
4991 Corporate Drive, Huntsville, AL 35805
TEL 866.277.1924 FAX 256.430.4030
www.avocent.com

Avocent, the Avocent logo, The Power of Being There, DSR, DSView and Cyclades are registered trademarks of Avocent Corporation or its affiliates. All other marks are the property of their respective owners. Copyright (c) 2007. Avocent Corporation. All rights reserved.

0207-BC-WP