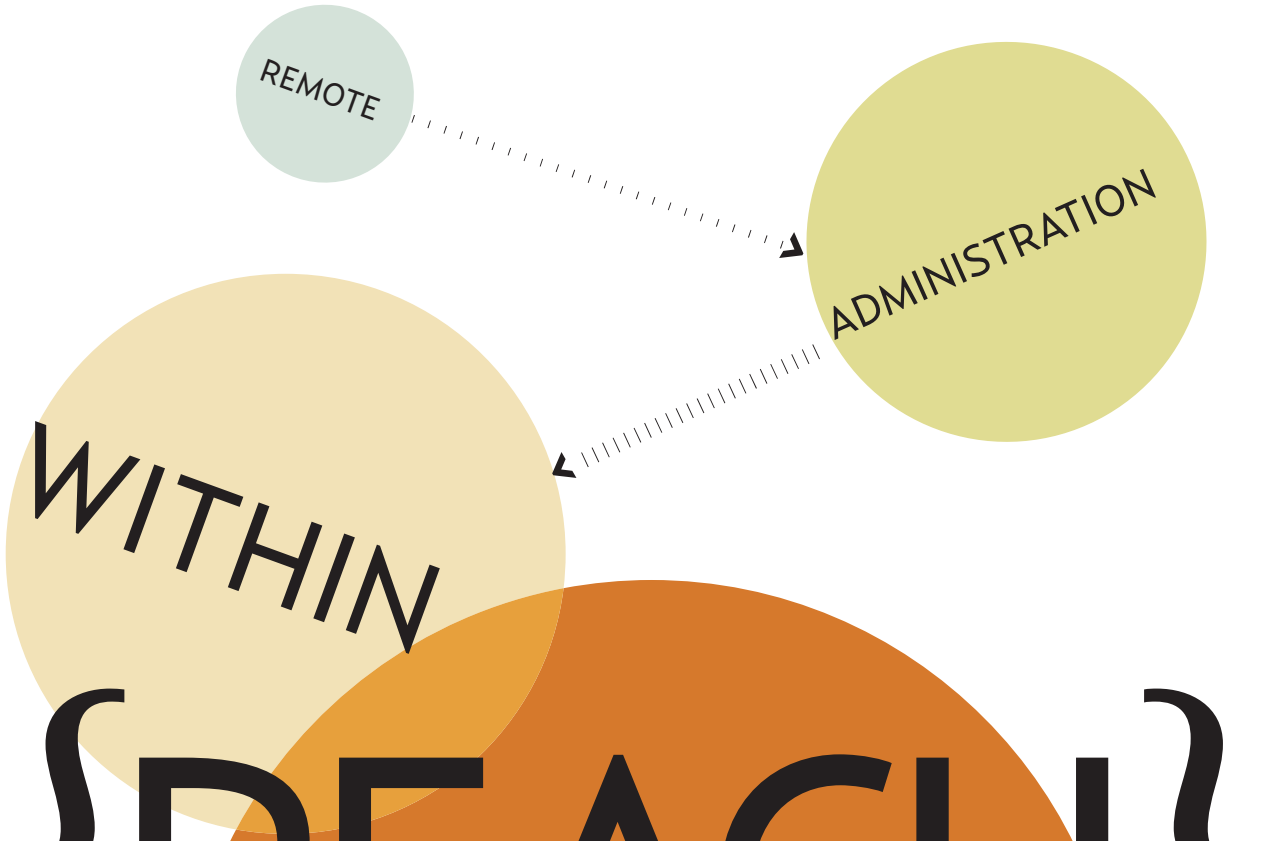
CMP
United Business Media

Network Computing®

APRIL 16, 2007 WWW.NWC.COM

For IT By IT



{REACH}

Long-distance server repairs got you down? Invest in a true OBM system to see uptime soar / BY STEVEN HILL

IT NEVER FAILS. After a 50-hour week you finally settle down for a quiet Saturday with the spouse and kids—a good movie and a big bowl of popcorn—and your beeper goes off. The system is completely down at a branch office 100 miles away, a terminal session just won't work, and there's much wailing and gnashing of teeth among the employees trying to get work done.

Unfortunately, even the best in-band remote-management tools live and die with the status of your network, and if it's unavailable, the only option is to saddle up your pony and ride.

Vendors are pushing system-management processors as a way of giving you complete remote control of the server. They're even working up standards like SMASH/IPMI (Systems Management Architecture for Server Hardware/Intelligent Platform Management Interface) to further that mission. But these are only partial solutions because they're ineffective if the main network is accessible. True OBM (out-of-band management) systems can reduce network downtime—and save you travel time—by providing some form of remote access to key systems regardless of the network's status.

OBM approaches include KVM-IP systems, SCSs (serial console servers) and intelligent remote power management. Although each approach has pros and cons, the first obstacle is usually obtaining budget. With the number of in-band remote-management platforms available, it may be hard to justify the added cost and complexity of a separate OBM system. Most system admins have been using RDP (Remote Desktop Protocol) and other in-band management tools for years, and these have worked well for the majority of remote problems, except in the rare instances when network connectivity is lost. The system redundancy being built into server and network hardware and the improved stability of OS software are making catastrophic failures far less common, thereby reducing the need for redundant OBM systems. But for those sites with stringent uptime requirements, options are wide-ranging.

IT'S ALL INSIDE

The big push in server technology is the use of an on-board system-management processor that can serve as a direct management interface. The premise is similar to the serial-management console used in many high-level network and storage systems, but with the richer features that are available over a Web GUI. In the past, many first-tier server vendors may have offered a basic interface to provides access to hardware functions regardless of the state of the OS.

Five key protocols govern remote-management interfaces. The most recent contenders are IPMI, SMASH, and WS-Management (Web Services Management). These newer protocols offer greater monitoring and management capabilities than their predecessors, SNMP and WBEM—(see "A SMASHing Success?" at *nwc.com/go/0416smash*)—but many vendors offer IPMI and SMASH support only to ensure cross-platform compatibility. They design their embedded management processors for improved integration with their own high-level enterprise-management products.

Most of the first-tier server vendors now provide for OBM with an integrated system-management processor

IMPACT ASSESSMENT: OUT-OF-BAND MANAGEMENT

	BENEFIT	RISK
IT Organization	OBM systems let administrators access servers, switches, routers and other devices when the primary network is inaccessible. Servers can even be power-cycled with the right OBM products.	An OBM system is another potential attack point, but the probability of that kind of attack is very low, considering the serial nature of most OBM solutions.
Business Organization	The business will benefit from faster troubleshooting and an elimination of drive-time lag for administrative staff, particularly at remote sites.	There are no real risks to the business.
Business Competitiveness	Time is money. The faster a company can recover from a systems failure, the more uptime it can offer customers.	OBM has no real business competitiveness downside.

BOTTOM LINE

For companies that have stringent uptime requirements or have multiple remote sites, an OBM system lets administrators bring crashed systems or networks back online without drive-time lag or on-site employee intervention. For more centrally organized enterprises or those that are more tolerant of lag before restoration of services, OBM may not be justifiable.

that offers enhanced capabilities beyond the basic functionalities offered by IPMI and SMASH. DRAC (Dell Remote Access Card), Gateway's GLO (Gateway Lights Out) systems, Hewlett-Packard's iLO (Integrated Lights Out) management processor, IBM's RSA (Remote Supervisor Adapter) and Sun Microsystems' ILOM (Integrated Lights Out Manager) have emerged as viable options for network-based remote-server management. These subsystems offer remote-management features, such as power cycling, CLI-based scripting, secure user authentication, event logging, console redirection and support for virtual storage media; include browser-based access independent of the OS status; and allow an ordered restart of a hung system.

For systems that don't offer an integrated management processor, American Megatrends markets the MegaRAC card (see "Bridging the Gap," below). For about $500, this PCI card can be used in legacy systems to provide a number of remote-management features available in newer systems. Although the MegaRAC card offers features like power control, video redirection and KVM-IP for older PCI-based systems, its environmental reporting capabilities are limited by what information is available from the OEM system and the interface it uses for that transfer.

Integrated system-management processors interact directly with the server's hardware, making them an excellent tool for OBM purposes, but these systems have been designed to communicate primarily over a dedicated or a shared Ethernet port. For these to be part of a true OBM solution, the service processors must be placed on a separate, high-availability network, with the accompanying per-port costs. Avocent has developed its MergePoint product to combine management port aggregation with multiplatform support and secure user authentication (see "MergePoint Fuses Port Aggregation, Multiplatform Support" at *nwc.com/go/0416mergepoint*). Most system-management processors also offer serial redirection of text-based CLI functions, but OBM access to these requires an additional serial console server to aggregate the connections to serial ports from multiple systems.

DIGITAL KVM-IP

An alternative to integrated system management is the use of KVMs. Originally, KVMs were simple switches that let multiple systems be run from a single location. Today, digital KVM systems offering KVM over IP use standard Category 5 cabling in combination with a small adapter that converts KVM—and even USB I/O—to the common IP protocol. This eliminates the bulky cables of earlier systems and lets KVM-IP signals run over conventional networking hardware.

To see how KVM-IP would work from an OBM perspective, we examined Avocent's latest 16-port DSR2030 KVM-over-IP switch. The company's DSR series supports Web-based KVM-IP, intelligent power distribution and serial console management of target devices, as well as secure modem access to managed systems for true OBM applications. In its base capacity, the DSR2030 supports IP-based KVM switching of servers locally using a directly attached monitor, keyboard and mouse. Remote Ethernet users also can access the DSR2030 using its secure, internal Web interface or through Avocent's server-based DSView 3 app, which supports the management of any number of DSR switches.

What takes the DSR series beyond basic KVM-IP functionality and into the realm of OBM solutions is its flexibility to directly connect to servers using KVM/USB modules, serial devices over separately powered serial modules and intelligent switched PDUs (power distribution units). More important, all these devices can be accessed through the Web—if network connectivity is available—or, in the event of total network failure, through a modem and the DSView software.

BRIDGING THE GAP

ALL YOUR NEW SERVERS have integrated system-management processors, but what can you do to remotely manage legacy systems that don't have that luxury? Long-time BIOS manufacturer American Megatrends' PCI-based MegaRAC G4 system-management processor card offers a variety of useful remote options for practically any PCI-capable system.

Available to both OEMs and IT customers, the MegaRAC G4 uses an on-board 266-MHz PowerPC RISC processor, 32 MB of SDRAM and 16 MB of flash memory to provide most of the capabilities of embedded management systems. The card fits in a standard 16-bit PCI slot and remains accessible regardless of system status, either by drawing power from the PCI bus or through an optional external power supply.

Cables connect the MegaRAC to motherboard jumpers to support remote reset and power cycling for USB over IP. There's also a custom Y-cable that provides VGA input to the card to support KVM-IP and console redirection of desktops with resolutions as high as 1,280x1,024. The system also supports virtual CD-ROM and floppy media as well as USB-based flash drives or hard disks.

Priced at about $500, the MegaRAC G4 may seem a little expensive, but it just might be one way to breathe new life into an aging system that's difficult to replace.

Even Avocent would be the first to admit that experiencing KVM over a modem would be like watching grass grow, but a number of key functions don't require the use of a remote desktop. For those that do, the latency of the remote user experience is perhaps the main downside to full KVM-IP access. The amount of traffic generated by redirecting an entire desktop over an IP link can make remote management tedious at less than T1 speeds, but the DSView UI supports multiple bit-depths and levels of compression to reduce the amount data traffic needed for desktop redirection. This is an issue not only with KVM-IP systems, but also with integrated solutions like system-management processors, as well as with almost any product that offers bitmapped—rather than text-based—console redirection.

Another interesting feature of KVM-IP setups: the availability of virtual storage media capabilities. For example, with a KVM-IP system, an administrator could configure a DVD or hard drive on his laptop to act as a local drive on a remotely managed system—a handy feature when you're in Chicago and a remote server in Milwaukee starts squawking for you to insert CD #2 to continue.

Avocent's DSR2030 provides its own integrated, authentication-based security to prevent unwanted access, and it supports external authentication services such as Active Directory, LDAP, RADUIS, TACACS+ and RSA SecureID. For environments requiring greater security, Avocent offers a NIAP-certified SwitchView SC KVM system that's been validated to meet EAL4 (Evaluation Assurance Level 4) for secure government applications. Although Avocent seems to be the only company offering this level of security, most other KVM-IP vendors—including Aten, HP, Lantronix, MRV Communications, Raritan and Rose Electronics—and even smaller-scale KVM-IP systems like those from Belkin and Minicom, offer varying degrees of secure and encrypted remote KVM-IP connectivity.

Of course, full KVM-IP for an OBM solution is a bit like the Cadillac of remote access, and the cost can run anywhere from $150 to $450 per managed machine. This may seem expensive, but the combination of base OBM connectivity and in-band management easily justifies the price when compared with the cost of service calls and downtime for systems in remote locations.

SERIAL CONSOLE SERVERS

When your needs are basic, but extend beyond simple power monitoring and cycling, OBM systems that use serial-based, device-level remote management may fit the bill. Although the current trend is toward sexy Web interfaces, almost every device in the enterprise—from the smallest switch to the largest SAN—offers a basic management interface in the form of a serial console. SCSs reach back to the very roots of IT management and allow the aggregation of multiple serial connections that can be managed over a single serial or Ethernet connection.

Early generations of these consoles focused on providing switched, text-based access to serial devices, but an increasing demand for remote system security and the need to monitor a greater variety of devices have changed the role of the SCS. To get an idea of the features available on the latest generation of SCSs, we had MRV send us products from its LX-4000T series of console servers. MRV sent a test package to our Real-World Labs® in Green Bay, Wis., that included an LX-4016T SCS and LX-5250 intelligent PDU.

Serial device connectivity continues to be the main focus of MRV's LX solution, but with the LX-4016T we

COMPARISON OF OBM APPROACHES

	PROS	CONS
Digital KVM-IP	Rich management features Full desktop presentation Accessible regardless of OS status BIOS-level access Supports serial access Optional modem connectivity Remote power-management options Clean system shutdown capabilities	GUI latency issues High cost Midlevel-to-high bandwidth requirements
Integrated system-management processors	Low cost Rich management features BIOS-level access Clean system shutdown capabilities Remote power management options	Midlevel-to-high bandwidth requirements Presents multiple points of management GUI latency issues
Intelligent remote-power management	Low cost Optional modem connectivity Optional staggered system power-up	Hard power cycling not optimal for servers Power-only management of attached devices
Serial console servers	Industrywide system support Low bandwidth requirements Easily scripted interface Low-to-moderate cost Optional modem connectivity Remote power-management options Clean system shutdown capabilities Environmental monitoring capabilities	Usually limited to low-level functions Primarily text-based

could set up a remote serial-management environment that included power management and serial device control, as well as support for environmental monitoring and a video camera system. Power was managed with the use of MRV's LX-5250 Power Control Series PDU, which offers load monitoring, independent port-access controls and sequential power-up capabilities. Fully functional as a standalone system, the LX-5250 can be managed directly over a Web interface or through a serial link to an LX-4000-series SCS.

LX-4000T-series console servers can support as many as 48 ports, and each system is designed to operate independently or in a clustered configuration with the addition of MRV's client-server MegaVision Pro network-management software. MegaVision Pro can offer single-pane-of-glass access to any number of SCSs, enabling remote access control over thousands of serial devices, PDUs and environmental monitors. In a standalone environment, MRV's LX-4016T provided very granular, port-level control over all attached devices through the company's integrated CLI or Web management system—without the need for additional software.

Considering the level of access these systems provide, security should be an overriding concern—a fact not lost on console vendors. The MRV LX-4000T series meets the FIPS 140-2 cryptographic security standard, is NEBS-certified, and offers support for SSH 2.0, SNMPv3, IPv6, RADIUS, SecurID, LDAP, TACACS+, PPP PAP/CHAP and PPP dial-back capabilities. MRV isn't alone in this space; SCSs with a wide matrix of management capabilities and similar security features are also available from HP, Perle, Lantronix, Cyclades (now Avocent), Raritan and Thinklogical, among others.

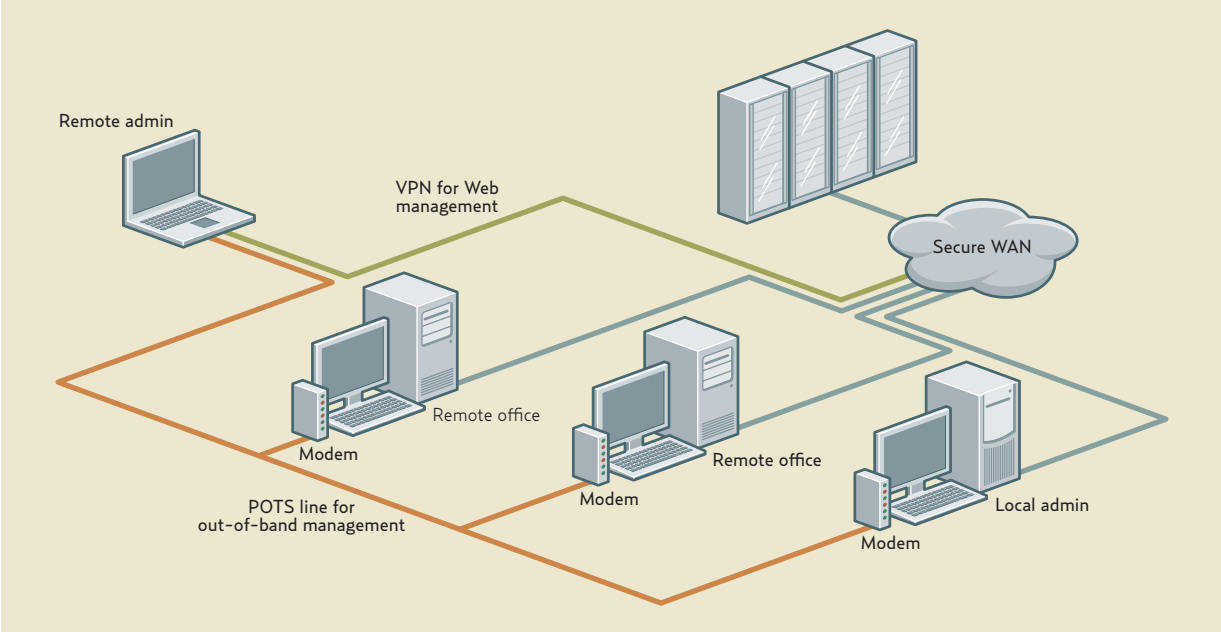
For most high-end networking, telecom and storage gear, a plain-old serial port is still the most common interface for communicating with an embedded management interface, but serial consoles are useful for managing many OSs as well. Serial-based terminal services have always been a capability of Unix variants and Linux, and with the introduction of Server 2003, Windows began offering its EMS (Emergency Management Services) support to provide baseline access to key Windows management options through the serial port.

From a pure OBM standpoint, dial-in access is supported by most SCS systems, but almost all modern SCSs use standard network connections as their primary method of communication to support a richer management environment, so access to SCSs is dependent on the status of your network. Depending on the required uptime of your systems, the possibility of creating a separate high-availability network for OBM should be explored—or, you should at least make provisions for remote telephone access to critical network equipment

INTELLIGENT REMOTE POWER MANAGEMENT

Remote power cycling is perhaps one of the easiest and

REMOTE DOORS TO THE SERVER



Most in-band and side-band management tools are **dependent on a functional network connection.** But modem-enabled devices, such as serial console servers, intelligent power distribution units and KVM-over-IP switches, can **use basic telephone connections** to provide connectivity when network devices or servers are inaccessible due to a network outage.

least expensive options available for OBM. Although this service is also available as a capability in many embedded switch- and server- management solutions, in many cases this function is managed through an Ethernet connection and, therefore, is out of reach if the network becomes inaccessible or if the device loses power. The most basic OBM solution—a remotely manageable, switching PDU—can be employed to report system power status and, if necessary, cycle the power on an unresponsive device.

Switched PDU modules are available from a wide variety of vendors and can be configured to support almost any conceivable combination of outlet, voltage and electrical load requirements. Although the features vary by vendor, these systems monitor incoming and output power status, and offer the ability to remotely cycle the power to specific devices. Many systems offer a Web browser interface for a detailed graphical display of system status, and some provide more advanced features like a sequenced power-up routine to restart firewalls, routers and switches in the appropriate order.

This type of power cycling is not the optimal solution for dealing with servers—when compared to a clean reboot—but it will do in a pinch. And though a fancy Web interface is all well and good, for more basic OBM capabilities there's still nothing like a simple modem and a dumb terminal to ensure connectivity through thick and thin. We know, the mere thought of dusting off your ancient USR Courier sends chills up your spine, but sometimes the most low-tech answer is the best.

REACH OUT AND BOUNCE SOMEONE

The conventional telephone network in the United States is one of the most reliable options available for true OBM connectivity to remote systems. Aside from those who've experienced major disasters like earthquakes and hurricanes, very few Americans can honestly admit to ever picking up the phone and not being able to make a call whenever they want, even when the power is out.

More important, POTS is available worldwide. There are still large areas of the United States that offer little or no reliable broadband accessibility, but POTS is almost always available, and for a fraction of the cost of other connectivity options. What makes POTS particularly useful for basic, power-level OBM is the limited amount of information that needs to move between the administrator and the managed device. Many systems use basic ASCII text or simple ANSI graphics for their serial interfaces, so very little bandwidth is required, and the remote experience is almost identical to that of a local connection.

In addition, basic remote power management has a relatively low cost—a managed PDU, phone line, modem and basic UPS could provide high-availability remote power control for 10 to 15 devices for less than $100 per device. Furthermore, data centers using more advanced power-management systems may also have inexpensive options that support modem-based remote power cycling. For example, American Power Conversion offers a simple OBM card that plugs into its high-end UPS devices to provide protected, terminal-based modem access to features in its power-management system.

FOCUS ON WHAT'S IMPORTANT

With all the options available for in-band system management at both hardware and software levels, basic monitoring and power control of key networking systems should be the primary consideration in any OBM strategy. The ability to remotely restore essential networking systems will allow more advanced in-band management solutions to become available. An OBM solution may not be necessary for every component, only those that impact the accessibility of others.

Given the heightened focus on data security, the importance of issues like user authentication, error logging, event-based alerts, system parameter monitoring and audit trails will vary from business to business, but vendors of the newest generation of OBM products have recognized the importance of protecting these remote systems, and there's no reason that a carefully planned OBM system should present more of a security risk than any other Internet-based activity.

Granted, these types of problems aren't as much of an issue in the typical data center environment. In larger installations there's someone on staff 24/7/365 who at least knows what to do during a serious emergency, but with the number of smaller distributed data centers appearing in branch offices, the simple ability to remotely power cycle a server or switch can mean the difference between a five-minute outage and a five-hour one. ■

STEVEN HILL /// is an NWC technology editor. Write to him at *shill@nwc.com*. Post a comment or question on this story at *nwc.com/go/ask.html*.