

Out-of-Band Management for Windows Server™ 2003

White Paper

Abstract

This paper provides information about out-of-band management for the Microsoft® Windows Server 2003 family of operating systems. It describes the capabilities of new Emergency Management Services, and guides systems administrators in designing and implementing out-of-band management facilities for their networks.

May 13, 2003

Contents

Introduction	2
In-Band vs. Out-of-Band Management	2
Emergency Management Services	2
Console Redirection	2
Special Administration Console	3
Is EMS Reliable?	4
Networking EMS	5
Making EMS Easy	6
Conclusions	6
Acronyms and Terms	7

Introduction

Many networked devices, such as UNIX servers, routers and switches, are accessible through local serial console ports, for initial configuration and emergency management. Today, “console management” is an integral part of the data center, allowing secure access to systems even when the network is unavailable. Until now, this functionality has not been available on Microsoft Windows® servers, which are traditionally managed with cumbersome KVM (keyboard, video and mouse) switches.

In Windows Server 2003, Microsoft introduced Emergency Management Services (EMS), a powerful suite of applications for out-of-band management. EMS enables true “headless” server operation, which significantly reduces hardware costs by eliminating the need for video cards, monitors, keyboards and mice during Operating System (OS) installation, operation and recovery.

This paper provides an overview of out-of-band management and EMS, and shows how to connect EMS ports to networks.

In-Band vs. Out-of-Band Management

By default, systems administrators use standard tools such as Terminal Services and Microsoft Management Console (MMC) to manage Windows servers through the network. These in-band tools require the target server to cooperate; if the server’s TCP/IP stack isn’t functioning, for example, there is no way to reach the server.

An out-of-band connection through a serial console port relies on only the most primitive of OS services. As long as the kernel is functioning, access to the system is possible – even if the network stack or user interface is down. And because the console port delivers only text data, it offers good performance over low-bandwidth connections such as dial-up lines. Out-of-band management is a reliable way to reach servers when things have gone wrong.

Out-of-band management doesn’t replace in-band management – it improves a system administrator’s ability to quickly respond to situations when standard tools aren’t available. Of course, faster response times translate to increased uptime.

Emergency Management Services

Emergency Management Services (EMS) is a suite of features spread over multiple elements of Windows Server 2003. Together, these applications enable remote management and system recovery through the server’s serial console port, even when the server is unavailable through the network. EMS consists of Console Redirection and the Special Administration Console.

Console Redirection

Console Redirection allows administrators to monitor and control the boot process by sending all system output to both the video adapter (if present) and the serial console port. Likewise, it accepts inputs from the console port, as well as the keyboard (if present).

During a server’s Power on Self-Test (POST), before Windows begins to load, Console Redirection is typically a function of the server’s BIOS.

EMS Console Redirection starts as soon as Windows begins to load, and is available until the Windows graphical interface becomes active. It has been integrated into a number of tools, including the setup loader, the text-based setup process, the recovery console, the loader and the Stop Error handler.

Once the Windows graphical interface is active, Console Redirection is no longer available, and EMS focuses on the Special Administration Console.

Note: Console Redirection is unrelated to COM port Redirection, which extends serial ports across networks. COM port redirectors are software drivers such as Digi International's patented RealPort® protocol.

Special Administration Console

The Special Administration Console (SAC) allows administrators to access and control the OS when standard remote management tools such as Terminal Services are unavailable. Since SAC is a kernel-level function, it remains accessible even after higher-level applications have ceased to respond because, for example, a misbehaving program has used all available memory.

SAC provides low-level emergency features, such as the ability to:

- Set the server's IP address during the initial install
- Reconfigure IP settings to regain in-band connectivity
- Reboot or shutdown the server
- List all used and available resources (physical memory, kernel memory, etc.)
- List all processes, kill them, limit memory usage or change their priority
- Create Command Prompt Channels, for access to the file system.
- Run text-based applications (e.g., traceroute, telnet, etc.)

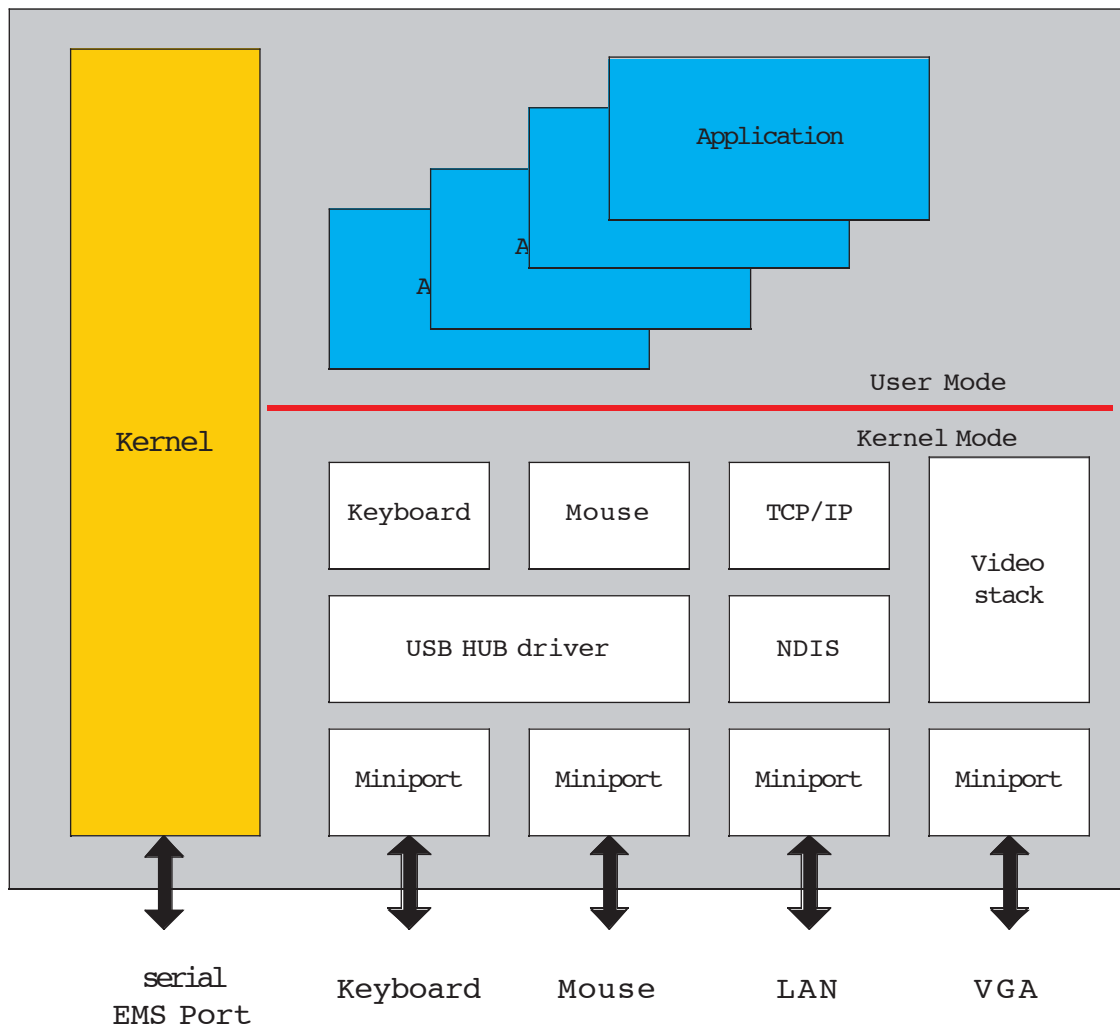
SAC provides the ability to analyze the logs and restart the server even after a Stop Error (AKA "Bluescreen"), though most other features will be disabled.

SAC is text-based and command-line driven, very much like DOS:

```
D:\WINNT\System32\telnet.exe
SAC>help
ch          Channel management commands. Use ch -? for more help.
cmd        Create a Command Prompt channel.
d          Dump the current kernel log.
f          Toggle detailed or abbreviated tlist info.
? or help  Display this list.
i          List all IP network numbers and their IP addresses.
i <#> <ip> <subnet> <gateway> Set IP addr., subnet and gateway.
id         Display the computer identification information.
k <pid>    Kill the given process.
l <pid>    Lower the priority of a process to the lowest possible.
lock       Lock access to Command Prompt channels.
m <pid> <MB-allow> Limit the memory usage of a process to <MB-allow>.
p          Toggle paging the display.
r <pid>    Raise the priority of a process by one.
s          Display the current time and date (24 hour clock used).
s mm/dd/yyyy hh:mm Set the current time and date (24 hour clock used).
t          Tlist.
restart    Restart the system immediately.
shutdown  Shutdown the system immediately.
crashdump Crash the system. You must have crash dump enabled.
SAC>
SAC>
SAC>
```

Is EMS Reliable?

Because EMS is a function of the kernel, and doesn't rely upon any drivers or applications, it is much more robust than either network-based management tools or KVM switches.



Network-based tools, such as Windows Terminal Services, require the server's TCP/IP stack to be running and require system memory.

KVM switches require keyboard, video and mouse drivers to be running and accessible.

To test EMS, we created a program that uses up all system memory, leaving the server functioning but acting very slowly. Pressing “<ctrl> <alt> <delete>” brought up the “Windows Security” screen, but a restart was not executed in a reasonable timeframe. Using SAC, we were able to kill the malicious process immediately and to restart the server.

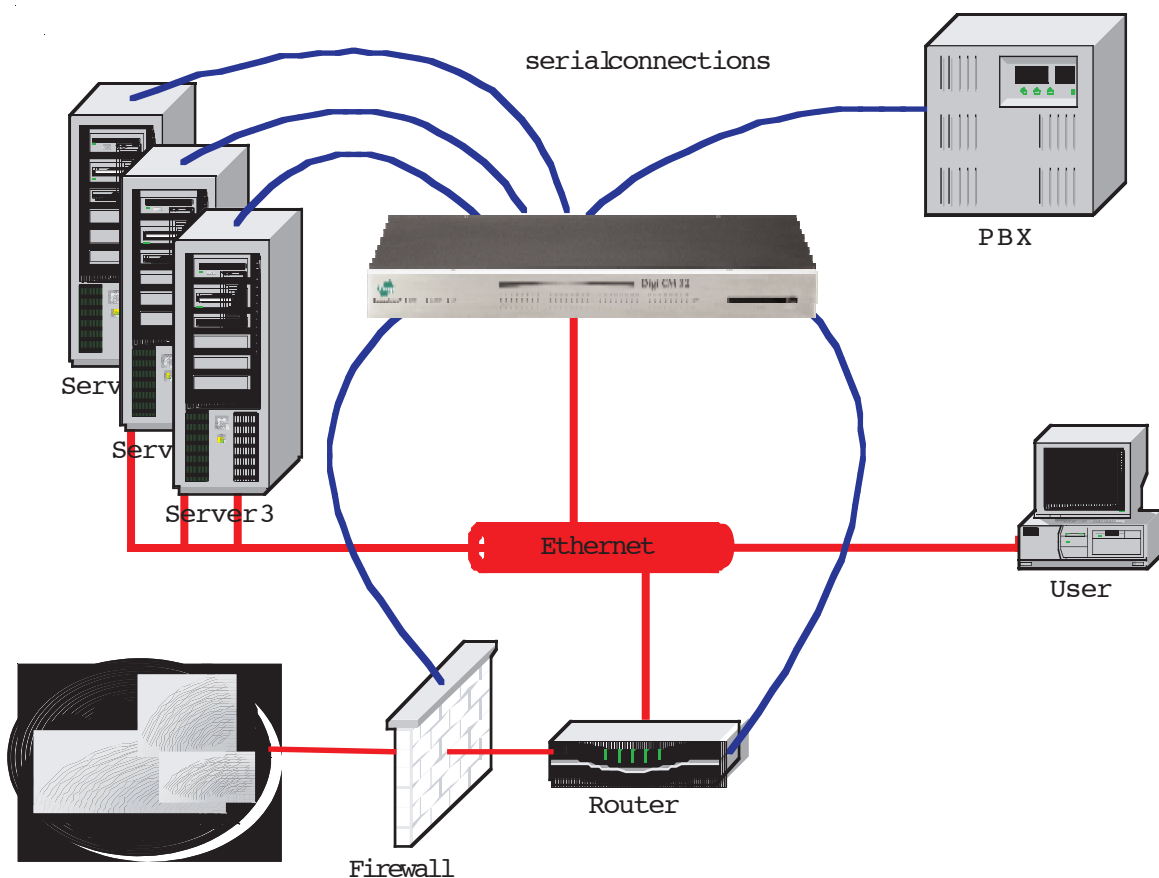
EMS offers much more reliable access than a KVM switch, and can quickly restore in-band management capabilities.

Networking EMS

The problem of easily connecting serial devices to networks was solved more than a decade ago. Terminal servers are standalone network devices featuring an Ethernet interface and multiple serial ports. They connect devices such as terminals and printers to the network without tying up valuable server resources. Typically, the serial devices are connected by telnet, or through COM port redirection software, such as Digi International's patented RealPort.

Note: Terminal Servers are unrelated to Terminal Services, which is a Windows application for in-band management.

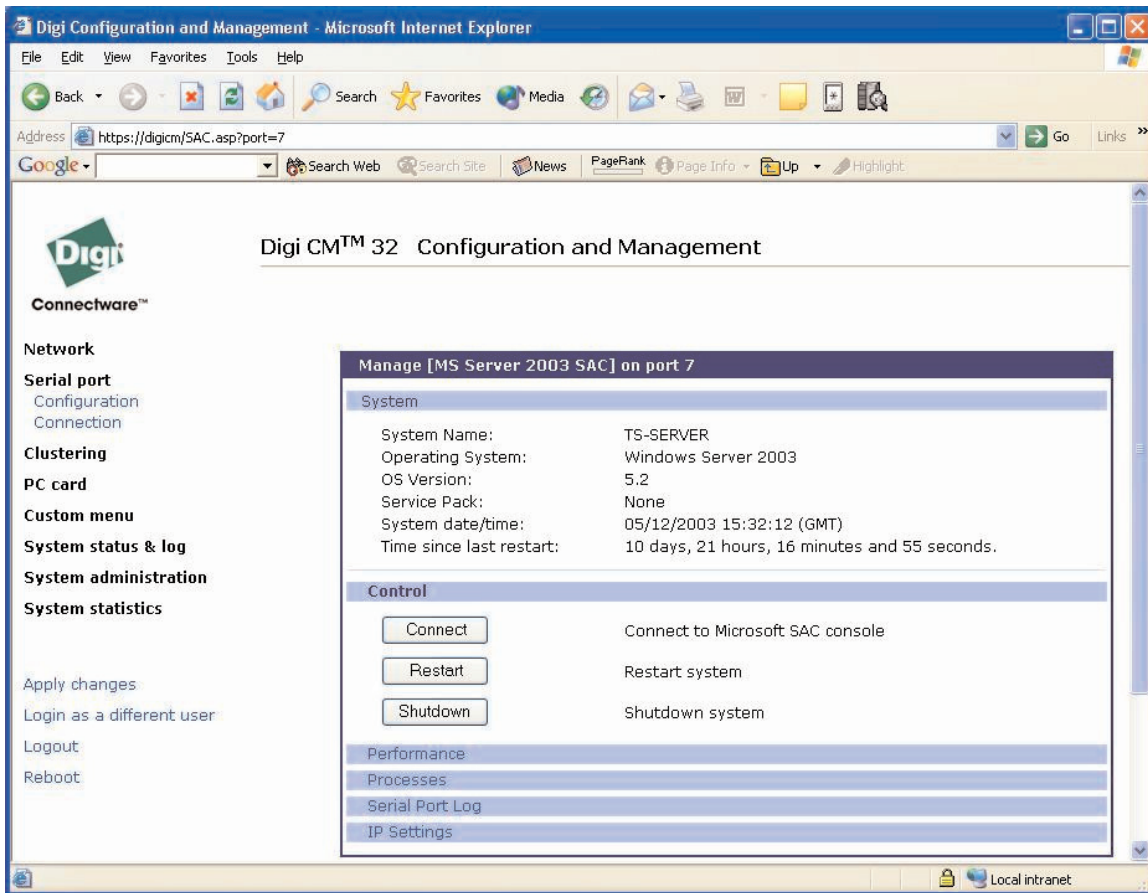
In the UNIX world, terminal servers are commonly used to provide access to the serial console ports for out-of-band management of servers, routers and switches. The console ports are connected to the terminal server, which is attached to the network switch, and optionally, a dial-up modem. Using telnet or SSH, the administrator can connect directly to a console port from anywhere on the corporate TCP/IP network, over the Internet, or through a direct dial-up connection.



Today's terminal servers are optimized for console port management. Encrypted SSHv2 has replaced the unsecure telnet connection, and all data exchanged with the console port is logged for troubleshooting and auditing purposes. The latest generation of terminal servers can also scan the console output for keywords and issue an SNMP trap or email message in case of an emergency. For ease of use, many terminal servers now offer a Web-based interface for configuration, and access to the connected servers, routers and other network devices.

Making EMS Easy

Windows administrators are accustomed to graphical user interfaces, rather than command lines. With that in mind, some new terminal servers have a browser-based point-and-click interface to SAC, which simplifies server management:



The browser-based front end makes SAC's functionality instantly available and reduces training time to a minimum. Additionally, HTTPS makes the SAC interface secure.

Conclusions

Out-of-band management is the reliable way to reach servers when things go wrong.

Emergency Management Services brings the benefits of out-of-band management to Windows Server 2003 systems, providing access to vital server functions over a low-bandwidth connection, even when the server's network stack and user interface are down.

By adding new Windows systems to terminal servers, one common technology can be used to reach any server, router or network device within a company, independent of its location or OS through a simple graphical user interface.

This approach consolidates and simplifies out-of-band data center management and can contribute to increased uptime and greater IT efficiency.

Acronyms and Terms

EMS	Emergency Management Services
HTTPS	Secure HTTP (Hypertext Transfer Protocol)
KVM	Keyboard, Video and Mouse switch
OS	Operating System
SAC	Special Administration Console
SNMP	Simple Network Management Protocol
SSH	Secure Shell

Digi International

11001 Bren Road E.
Minnetonka, MN 55343 USA
PH: 877-912-3444
952-912-3444
FX: 952-912-4952
Email: info@digi.com
www.digi.com

Digi International GmbH

Joseph-von-Fraunhofer Str. 23
D-44227 Dortmund
Germany
PH: +49-231-9747-0
FX: +49-231-9747-111
www.digi.de

Digi International (HK) Limited

Suite 1703-05, 17/F.
K Wah Centre
191 Java Road
North Point, Hong Kong
PH: +852-2833-1008
FX: +852-2572-9989
www.digi.cn

© 2003-2004 Digi International Inc.

Digi, Digi International, the Digi logo, Digi Connectware logo, Digi CM and RealPort are trademarks or registered trademarks of Digi International, Inc. in the United States and other countries worldwide. All other trademarks are the property of their respective owners.

91001238
B1/904



Connectware™