# Virtualization and Mobility in Client and Server Environments

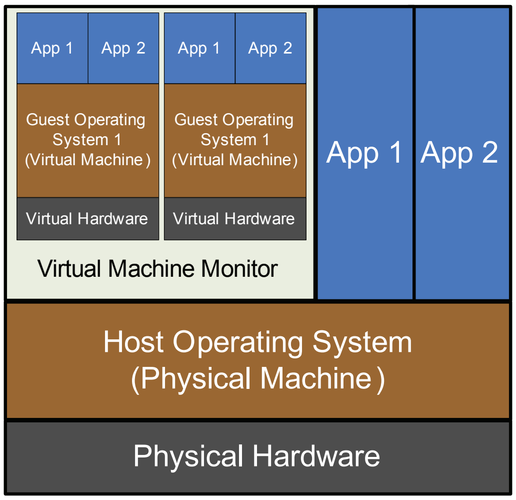
**Eduardo Correia**
*Christchurch Polytechnic Institute of Technology, New Zealand*

## INTRODUCTION

A great deal of popular software is not designed for mobility (Griffiths, 2004). This is peculiar because many mobile users expect to have easy access to an information infrastructure that links up their mobile phone, laptop, personal digital assistant (PDA), and other devices, while the backend systems of organizations need to be agile, especially as the number, range, and diversity of services and associated technologies grow. Enter virtualization, a technology that has been part of computing for many years, but only fairly recently become mainstream (Intel, 2006; Singh, 2004). It makes use of a virtual machine monitor (VMM), a mechanism that frees up systems from many of the physical constraints of hardware, by adding a software layer that abstracts hardware, so that an entire machine, operating system, applications, and even data can be stored as a set of standard folders and files. While it is well established that this architecture enhances security and reliability (Rosenblum & Garfinkal, 2004), it also enables both users and systems, as this article shows, to be mobile and responsive to change, both in client and server environments.

VMware Workstation, Microsoft Virtual PC, and other virtualization software takes the form of a standard application that can be installed on physical computers. As Figure 1 shows, these applications provide a VMM, which enables one system (the guest) to run within the context of another system (the host). The VMM presents a complete set of virtual hardware to each guest virtual machine (VM) running within this environment. Just as ordinary computers access physical resources, such as memory, processors, hard disks, and network adapters, so too do each of the virtual or guest systems, only their hardware is an instance of a generic abstraction that the VMM generates for each of them. The VMM then mediates various calls made by VMs to access the physical hardware of the host machine. Whereas the standard computer has a single operating system with applications installed to it, a computer with virtualization software runs, in addition, within the VMM one or more operating systems, each with their own applications installed.

*Figure 1. Virtualization architecture*


App 1
App 2
App 1
App 2
Guest Operating System 1 (Virtual Machine)
Guest Operating System 1 (Virtual Machine)
Virtual Hardware
Virtual Hardware
Virtual Machine Monitor
App 1
App 2
Host Operating System (Physical Machine)
Physical Hardware

## MOBILE VIRTUAL MACHINES

While virtual private networks enable users to work from remote locations, as if they are sitting at a machine on the local network to some extent, this approach has certain drawbacks. Users may wish to connect with machines that do not belong to the organization and therefore do not adhere to its policies and standards. Antivirus software may be out of date or updates not installed, for example. One solution is to provide a quarantine area that will allow a machine into the network, but restrict its access to resources until certain criteria have been met. Cisco Systems' Network Admission Control (NAC) and Microsoft's Network Access Protection (NAP) are examples of this kind of solution (Conry-Murray, 2005). Alternatively, network administrators can make use of the VMware Assured Computing Environment (ACE) to produce and deploy secure, fully built virtual machines that apply custom policies and adhere to certain specified standards (Burt, 2004).

The fact that it is in effect the VM that forms part of the network and not the physical machine means that it does not matter to the network administrators that these particular hosts may not have the latest antivirus signature files or applied recent updates, as this underlying (physical) system does not interact with the network and cannot influence it in any way. Naturally, the user's physical machine could fail causing the VM itself to fail, but this will still not affect the network, and restoring the client machine is simply a matter of copying the ACE VM from removable media, such as DVD or a pen drive (VMware, 2006a). In this way anyone needing temporary access to the network can be given it because perhaps the only way of accessing it using their own machine is through a VM compliant with the standards set by the organization, including exactly which resources can be accessed and the length of time the VM can be used.

## SYSTEM AND SESSION MIGRATIONS

When conventional systems need to be moved from one set of hardware to another, the operating system and server applications first need to be installed and then the data, assuming it is on the same system, moved, either by simply copying it or restoring it from a backup. It is not just that this is a time-consuming exercise, but also it often entails having to navigate the complexities of making a system work with significantly different hardware, and its associated drivers and other software. This can cause lengthy outages and make system migrations complex and arduous. Virtual systems, by contrast, always access the same set of physical resources the VMM presents to it, whatever the differences in the actual underlying physical hardware, making them much more mobile than conventional systems. In fact, moving the entire system is simply a matter of copying data from one (physical) machine to another, making VMs highly portable (Wolf & Halter, 2005, p. 481). With Vmotion, systems administrators can even move virtual machines without interrupting service availability (VMware, 2006b), something that has been used with success in live production environments (Rosenkoetter, 2006). This makes it feasible to apply many changes during business hours that would otherwise have been scheduled for weekends or at least when the network is quiet (Cline, 2006).

In such cases virtualization enables easier migration of systems from one set of hardware to another, and significantly reduces the risk associated with such change. This risk is reduced further by the ease with which it is possible to store multiple older versions of virtual systems. Where for instance poor software or problematic devices are installed, virtualization enables administrators to return the machine easily to a selected previous state. This concept can be taken a step further by capturing and virtualizing a client's entire session with an existing server, then migrating to another system that is the same or different, such as from a desktop machine to a PDA (Baratto, Potter, Su, & Nieh, 2004). In fact virtualization can even be used by mobile users to "decouple" a computer into a "body (display, CPU, RAM, I/0) and a soul (session state, software, data, preferences)" so that a user with a portable device can walk up to any computer and resume a session started on another machine (Cáceres, Carter, Narayanaswami, & Raghunath, 2005, p. 65).

## CONCLUSION

Virtualization has expanded dramatically in recent years because it is a flexible, scalable technology. It allows powerful hardware to be used more efficiently by distributing the processing, storage, and movement of data among several virtual systems that can still make use of clustering and other conventional forms of load balancing and redundancy. VMware ESX Server and Microsoft Virtual Server for instance make it cost effective to host a single major application per server, so reducing software conflicts and increasing reliability by isolating each of the guest systems, as well as the host from one another while enabling systems administrators to fine tune systems to resident applications. It also makes it easy to retain (copies of) entire systems either for the purposes of disaster recovery or to test future development, perhaps with a view to implementing such changes on production systems.

Virtualization can be utilized in a range of situations in both client and server environments, be it as part of a mission-critical system users connect to; a disaster-recovery infrastructure; a gateway for connecting securely to the network; a deployment of secure, fully built clients that comply with specified standards; or a portable learning environment comprising an entire network of virtual machines that may or may not be connected to virtual and even physical switches, but which can be easily moved from one physical machine to another. It is true that virtualization often demands powerful hardware in order for it to cope with the demands of hosting numerous systems; but with the reduction in the cost of hardware, the use of virtual systems becomes a viable proposition for organizations, especially as they are easier to manage and more agile than conventional systems. It is no wonder then that manufacturers are beginning to produce hardware that is designed with virtualization in mind (Intel, 2006), and that VMware and Virtual PC have become such well-known brands in recent times. According to one survey, respondents expected 45% of new servers deployed this year to make use of virtual machines (IDC, 2005), a trend, it appears, that is set to continue.

## REFERENCES

Baratto, R. A., Potter, S., Su, G., & Nieh, J. (2004, September 26-October 1). MobiDesk: Mobile virtual desktop computing. *Proceedings of the 10th Annual International Conference on Mobile Computing and Networking,* Philadelphia.

Burt, J. (2004, September 20). *VMware takes virtual machines mobile.* Retrieved April 5, 2006, from http://www.eweek.com/article2/0,1895,1647632,00.asp