Hosted virtual machines are typically used for desktop virtualization: they allow a user running, say, Mac OS X to run Linux in a window on her desktop. This is useful for running applications that are not available for the host operating system, and the performance hit is less noticeable when using interactive applications. Native virtualization is more suited to a server setting, where both raw performance and predictability are critical.
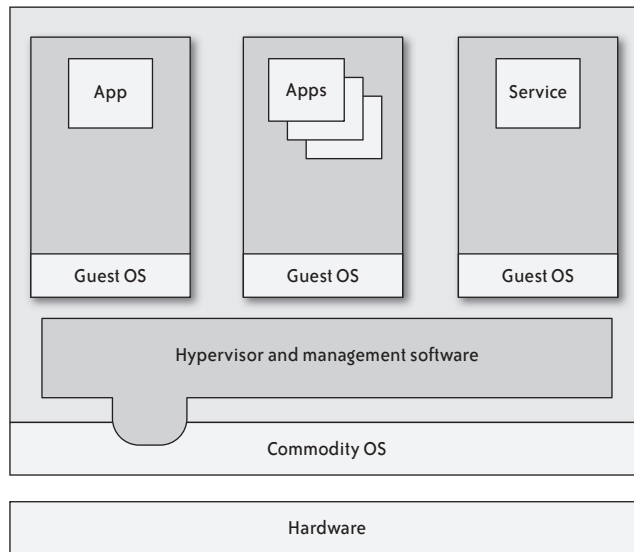

FIGURE 7-5. Hosted virtualization system architecture

When designing the Xen architecture, a primary concern was separating policy from mechanism wherever this was feasible. The hypervisor was designed to be a thin layer that managed the low-level hardware, acting as the reference monitor and scheduler and multiplexing access to hardware devices. However, since the hypervisor runs at the highest privilege level (and a bug here could compromise the whole system), the higher-level management is delegated to domain zero.

For example, when creating a new virtual machine, the bulk of the work is done in domain zero. From the hypervisor's point of view, a new domain is allocated, along with a portion of physical memory, some of that memory is mapped (in order to load the operating system), and the domain is unpaused. Domain zero takes care of admission control, setting up virtual devices, and building the memory image for the new domain. This split was particularly useful in the development process, as it is much easier to debug the management software in domain zero than the hypervisor. Moreover, it allows support for different operating systems to be