Мищериков Е.В., Хмелевской Б.Г. Принципы аппаратной виртуализации. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей VIII Всерос. научно-техн. конф. – Пенза: ПДЗ, 2008. – С. 120-122.

ПРИНЦИПЫ АППАРАТНОЙ ВИРТУАЛИЗАЦИИ

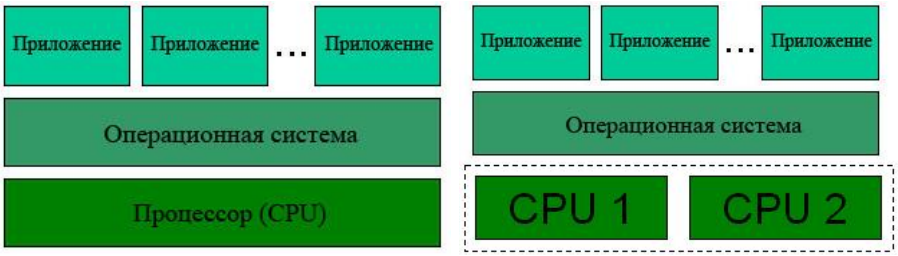
Е.В. Мищериков, Б.Г. Хмелевской

Пензенский государственный университет,
г. Пенза

Развитие рынка технологий виртуализации за последние несколько лет произошло во многом благодаря увеличению мощности аппаратного обеспечения, позволившего создавать по-настоящему эффективные платформы виртуализации как для серверных систем, так и для настольных компьютеров. Данные технологии позволяют запускать на одном физическом компьютере несколько виртуальных экземпляров операционных систем в целях обеспечения их независимости от аппаратной платформы и сосредоточения нескольких виртуальных машин на одной физической.

Аппаратная виртуализация является логическим продолжением эволюции уровней абстрагирования программных платформ – от многозадачности до уровня виртуализации.

Многозадачность является первым уровнем абстракции приложений. Каждое приложение разделяет ресурсы физического процессора в режиме разделения исполнения кода по времени.



МНОГОЗАДАЧНОСТЬ HYPERTGHREADING

HyperThreading – в широком смысле также представляет собой аппаратную технологию виртуализации, поскольку при ее использовании в рамках одного физического процессора происходит симуляция двух виртуальных процессоров в рамках одного.

Виртуализация представляет собой эмуляцию нескольких виртуальных процессоров для каждой из гостевых операционных систем. При этом технология виртуального SMP позволяет представлять несколько виртуальных процессоров в гостевой ОС при наличии технологии HyperThreading или нескольких ядер в физическом процессоре.

Программная виртуализация в данный момент превалирует над аппаратной ввиду того, что долгое время производители процессоров не могли должным образом реализовать поддержку виртуализации. Процесс внедрения новой технологии в процессоры требовал серьезного изменения их архитектуры, введения дополнительных инструкций и режимов работы процессоров. Несмотря на то, что программные платформы весьма продвинулись в отношении быстродействия и предоставления средств управления виртуальными машинами, технология аппаратной виртуализации имеет некоторые неоспоримые преимущества перед программной:

Упрощение разработки платформ виртуализации за счет предоставления аппаратных интерфейсов управления и поддержки виртуальных гостевых систем. Это способствует появлению и развитию новых платформ виртуализации и средств управления в связи с уменьшением трудоемкости и времени их разработки.

Возможность увеличения быстродействия платформ виртуализации. Поскольку управление виртуальными гостевыми системами производится с помощью небольшого промежуточного слоя программного обеспечения (гипервизора) напрямую, в перспективе ожидается увеличение быстродействия платформ виртуализации на основе аппаратных техник.

Возможность независимого запуска нескольких виртуальных платформ с возможностью переключения между ними на аппаратном уровне. Несколько виртуальных машин могут работать независимо, каждая в своем пространстве аппаратных ресурсов, что позволит устранить потери быстродействия на поддержание хостовой платформы, а также увеличить защищенность виртуальных машин за счет их полной изоляции.

Отвязывание гостевой системы от архитектуры хостовой платформы и реализации платформы виртуализации. С помощью технологий аппаратной виртуализации возможен запуск 64-битных гостевых систем из 32-битных хостовых систем с запущенными в них 32-битными средами виртуализации.

При разработке производителям процессоров пришлось изменить архитектуру за счет введения дополнительных инструкций для предоставления прямого доступа к ресурсам процессора из гостевых систем. Процессор с поддержкой виртуализации может работать в двух режимах – root operation и non-root operation. В режиме root operation работает специальное программное обеспечение, являющееся «легковесной» прослойкой между гостевыми операционными системами и оборудованием, – монитор виртуальных машин, носящий также название гипервизор. Чтобы перевести процессор в режим виртуализации, платформа виртуализации должна вызвать определенную инструкцию и передать управление гипервизору, который запускает виртуальную гостевую систему уже своими инструкциями (эти инструкции являются точками входа в виртуальную машину).