Enhanced Virtualization on Intel® Architecture-based Servers

Improve Utilization, Manage Change, Reduce Costs

Server virtualization on Intel® processor-based platforms is already helping businesses consolidate servers, simplify test and development environments, reduce total costs, and respond more quickly to shifting workload requirements. Intel® Virtualization Technology will provide fundamental architectural support for today's software-only solutions. It will increase the benefits of virtualization by fueling faster innovation and enabling virtualization solutions that are more robust, interoperable, and supportable.

March 2005

Table of Contents

Executive Summary

> *"…enterprises should be evaluating virtualization technology NOW."*
>
> – *The Future of Server Acquisition and Deployment,*
> Andrew Butler, Vice President & Research Area Leader,
> Server Technologies, Gartner, March 18, 2004.

Virtualization technology is already transforming the way many IT organizations provision and manage their systems and applications. Server virtualization enables the flexible and secure consolidation of multiple operating systems and applications onto a single platform. This helps to reduce server proliferation, increase utilization, simplify IT infrastructure, and reduce management costs. When used in conjunction with rapid software provisioning tools, it can also enable flexible and dynamic management of hardware resources to address shifting workload requirements. These capabilities are delivering substantial value for many businesses, and adoption is expected to increase dramatically over the next few years. According to estimates from IDC, 8 percent of servers shipped with provisioning and virtualization features in 2003, and the number will grow to 40 percent in 2007.[1]

Intel® Virtualization Technology, formerly known as Intel Vanderpool technology, will deliver hardware support designed to increase the value of today's software-only virtualization solutions. This extension to Intel architecture will help IT organizations:

- Reduce the cost and risk of implementing server virtualization solutions.
- Increase the reliability, availability, and security of applications running in virtual partitions.
- Improve interoperability with legacy software.

Intel Virtualization Technology will also simplify the development of virtualization software, which will fuel faster innovation. The specification has already been released. Hardware support in Intel® Itanium® 2 processor-based platforms is expected in 2005; support in 64-bit Intel® Xeon™ processor-based platforms is expected in the first half of 2006. Intel is now working with leading third-party vendors to accelerate the delivery of next-generation virtualization software that can make efficient use of this new architectural enhancement.

Virtualization is a transformative technology, and Intel is committed to delivering market-leading virtualization capabilities on Intel architecture. These capabilities will complement a variety of other Intel platform innovations focused on addressing some of today's most critical IT challenges. Together, these technologies will continue to improve the flexibility, reliability, security, and manageability of Intel architecture to deliver increasing business value across a wide range of IT requirements.

[1] Source: IDC Adaptive Resource Management Report (2004).

The High Cost of IT Operations

> *"Enterprises that do not leverage virtualization will pay up to 40 percent more in acquisition costs by 2008, and roughly 20 percent more in administrative costs…"*
>
> – *The Future of Server Virtualization*, T. Bittman, Gartner Research Note, July 17, 2003.

A typical IT organization allocates 70 to 80 percent of its budget simply to managing existing systems and applications.[2] One source of these costs is the large number of underutilized servers in the average datacenter. In the past, IT organizations have tended to host just one application per server. Given the affordability of industry-standard servers, this was a cost-effective strategy that simplified deployment and reduced potential software conflicts. Yet server numbers have increased worldwide by nearly 150 times in the past decade, and so have the costs associated with maintaining these systems.[3]

Average server performance has also increased. Today's servers are ten times more powerful than those of a decade ago. Virtualization helps IT organizations take advantage of this extra power by consolidating multiple applications and operating systems onto a single platform, to increase server utilization and reduce management, power and cooling requirements.[4] Today's solutions also enable flexible allocation of resources to handle unexpected workloads. With these tools, many IT organizations will find they can reduce their server-related costs (both capital and operational), while simultaneously improving datacenter agility (Figure 1).

VMware, a leading developer of server virtualization software, cites dramatic customer savings in server Total Cost of Ownership (TCO) via virtualization and consolidation:[5]

- Hardware cost reductions: 28-53%
- Operations cost reductions: 72-79%
- Overall cost reductions: 29-64%

VMware also cites up to 20 percent savings in software licensing costs.[6] With benefits of this magnitude, it is little wonder that server virtualization technologies are expected to be widely adopted over the next few years.

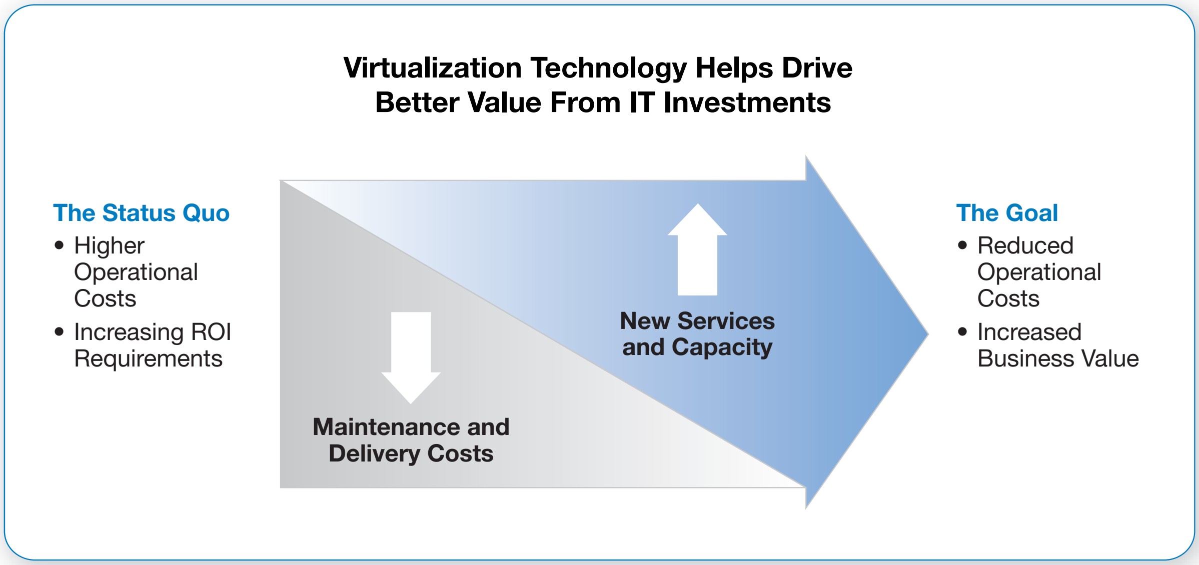

Virtualization Technology Helps Drive Better Value From IT Investments
The Status Quo
• Higher Operational Costs
• Increasing ROI Requirements
New Services and Capacity
Maintenance and Delivery Costs
The Goal
• Reduced Operational Costs
• Increased Business Value

Figure 1. Most IT organizations currently devote a significant majority of their resources to maintaining existing systems and applications. Server virtualization and consolidation can help to increase utilization, simplify the environment, and reduce total costs, which frees up funds for new projects that directly increase the business value of IT.

[2] Based on a quote by Kevin Rollins, President and COO, Dell Corporation, as reported in Dell and Sun Offer Different Visions, InformationWeek.com, by Larry Greenemeier, September 17, 2003.

[3] "Although processing power is relatively inexpensive (and getting cheaper), space, power, installation, integration and administration are not inexpensive..." Source: *The Future of Server Virtualization*, T. Bittman, Gartner Research Note, July 17, 2003.

[4] Note: There are several kinds of server virtualization, including OS emulation (e.g., a Java Virtual Machine) and workload management (multiple applications sharing an OS). This paper focuses on Resource Management, which enables multiple OS instances to share platform resources. For more information about other virtualization models, see *The Future of Server Virtualization*, T. Bittman, a Gartner Research Note, July 17, 2003.

[5] For details, visit the VMware Web site at: http://www.vmware.com/solutions/consolidation/mission_critical.html.

[6] Source: Michael Mullany, vice president of marketing at VMware, as referenced by Mark Hall in his article, *MAC Attracts New Support From…*, Computerworld, January 10, 2005; available at http://www.computerworld.com/softwaretopics/os/macos/story/0,10801,98824,00.html.

Virtualization—A Transformative Technology

> *"Virtualization enables firms to uncouple logical units of usage, such as an operating system or a storage volume, from physical units of operation, such as a server or a disk. This allows firms to maximize utilization—and gain great flexibility in moving and managing assets."*
>
> – *Organic IT 2004: Cut IT Costs, Speed Up Business*, Frank E. Gillett, Forrester Research, May 18, 2004.

In general terms, virtualization abstracts software from the underlying hardware infrastructure. In effect, it cuts the link that ties a specific software stack to a particular server. This enables more flexible control of both hardware and software resources, which can deliver value across a wide range of IT requirements (Figure 2).

Consolidating and Standardizing Server Infrastructure

Today's virtualization solutions support consolidation across the full range of Intel processor-based platforms. They can be used to increase utilization for small 2-way servers, or to support dozens of legacy applications on 4-, 8-, 16-way or larger platforms.

Platform resources—such as processing power, memory, I/O and storage—can be allocated and prioritized as needed based on business and application requirements. This is important since applications may have very different workload requirements. Flexible resource allocation can improve performance, increase consolidation ratios, and deliver better value for new platform purchases.

By enabling diverse operating systems to run on a common platform, virtualization also makes it easier to establish an enterprise-standard hardware infrastructure. Combined with consolidation, this offers fundamental benefits in simplifying the datacenter environment and reducing TCO.[7]

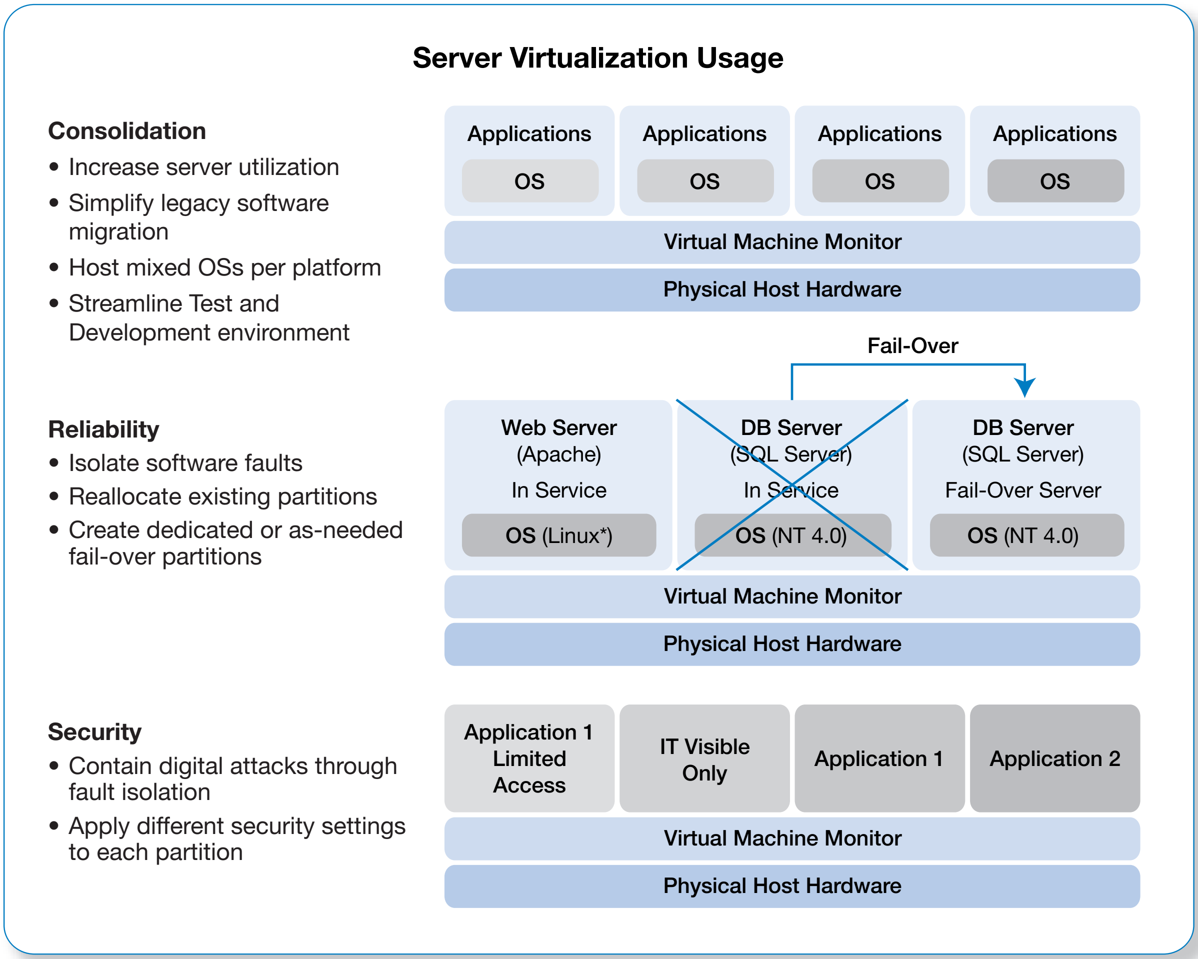

Server Virtualization Usage
Consolidation
• Increase server utilization
• Simplify legacy software migration
• Host mixed OSs per platform
• Streamline Test and Development environment
Applications
OS
Applications
OS
Applications
OS
Applications
OS
Virtual Machine Monitor
Physical Host Hardware
Reliability
• Isolate software faults
• Reallocate existing partitions
• Create dedicated or as-needed fail-over partitions
Fail-Over
Web Server (Apache)
In Service
OS (Linux*)
DB Server (SQL Server)
In Service
OS (NT 4.0)
DB Server (SQL Server)
Fail-Over Server
OS (NT 4.0)
Virtual Machine Monitor
Physical Host Hardware
Security
• Contain digital attacks through fault isolation
• Apply different security settings to each partition
Application 1 Limited Access
IT Visible Only
Application 1
Application 2
Virtual Machine Monitor
Physical Host Hardware

Figure 2. Server virtualization can be used to improve server utilization, reliability, and security, while simultaneously increasing business agility and reducing operational costs.

[7] For a detailed discussion, see *The Role of Standardization in Simplifying IT Infrastructure, an IDC Executive Brief*, September 2004.

Improving Availability and Security

Virtualization supports high availability and security in several key ways.

- **Fault Isolation**—Most application failures are caused by software faults. Virtualization provides logical isolation between virtual partitions, so a software fault in one partition is very unlikely to impact an application in another partition. Logical isolation also helps to contain digital attacks, which improves security in consolidated environments.
- **Fail-Over Flexibility**—Virtual partitions can be configured to provide automatic fail-over for one or more applications. Given the high availability features now supported in platforms based on the Intel Itanium 2 processor and the Intel Xeon processor MP, service level requirements can often be met by providing a fail-over partition on the same platform as the primary application. If even higher availability is required, the fail-over partition can be hosted on a separate platform.
- **Differential Security**—Different security settings can be implemented for each virtual machine, allowing IT organizations to maintain a high level of control over end-user and administrative privileges.

Simplifying OS and Hardware Migrations

A key advantage of virtualization is that it simplifies the migration of legacy applications onto new platforms to increase performance, reliability, and manageability. Instead of migrating the application onto a new operating system, it can be hosted with the existing operating system in a virtual partition on the new platform, with no need for software modification. This strategy can often be used to extend the useful life of legacy applications at relatively little cost and with less risk.

Streamlining Test and Development

Virtualization offers similar advantages for development and test environments. Successive iterations of the software stack, including the production version, can be hosted in separate virtual partitions on the same platform. This can improve hardware utilization and simplify lifecycle management. In many cases, IT organizations may be able to test new and upgraded solutions on existing production platforms, without disrupting the production environment. This not only simplifies migration but can further reduce costs by eliminating the need for duplicate environments.

Increasing Business Agility

It is far easier to provision or re-size a virtual partition than to purchase and deploy a new hardware platform. Today's automated provisioning solutions add to this advantage, and can dramatically improve IT responsiveness. Businesses can deploy fewer platforms, and use them more flexibly to address volatile requirements.

A New Era of PC Flexibility

Virtualization for Desktops and Workstations

Intel® Virtualization Technology will also be integrated into client platforms, with support expected to begin in 2005. Key benefits include:

- **Enhanced Availability and Manageability**—Critical IT management and network security tools can be isolated in secure partitions to prevent unauthorized tampering, to improve availability and recovery capabilities, and to enable upgrades, maintenance, and administration without interrupting end-users. These capabilities will complement the benefits of Intel® Active Management technology, which will be delivered in approximately the same time frame (for more information, see http://www.intel.com/technology/manage/iamt/).
- **Better PC Security**—Virtual partitions can be used to restrict access to personal desktops in multi-user machines, and to contain digital attacks (viruses, worms, hackers, etc.). For example, Internet browsing and e-mail access could be performed in isolated partitions to protect business applications and data from potential attacks.
- **Greater IT Flexibility**—Multiple users can be supported in secure, isolated partitions on a single PC; and multiple OSs can be deployed to support different functions (e.g., Unix for engineering applications; Windows for personal productivity suites). Personal and business applications can also be hosted on the same machine, and isolated to maintain high security and availability.
- **Desktop Portability**—A user's desktop can be encapsulated, and easily transferred to a secure, virtual partition on any other PC.

Datacenter in a Box

Virtualization for Small- and Medium-Size Businesses

Currently, server virtualization is most common in enterprise datacenters. Over time, it is likely to become equally popular among smaller businesses. It will allow them to simplify deployment and improve reliability, availability, and security by isolating applications in virtual partitions. Fail-over partitions can be configured to further enhance availability, and capacity can be scaled very flexibly by adding partitions or reallocating platform resources. As a business grows and more hardware capacity is needed, applications can be encapsulated and easily migrated into virtual partitions on new systems.

Server Virtualization on Intel Architecture

> *"Intel server utilization rates will double between 2003 and 2008."*
>
> – *Predicts 2004: Server Virtualization Evolves Rapidly*, T. Bittman, Gartner Research Note, November 14, 2003.

Virtualization software is available today from VMware* and Microsoft*, providing Intel architecture-based servers with capabilities that were previously available only on mainframes. Many businesses are achieving 20-to-1 or even 30-to-1 consolidation ratios by moving legacy applications onto 4-way to 16-way Intel processor-based platforms.[8]

Virtualization will become increasingly important as Intel dual-core processors enter the marketplace. In conjunction with Hyper-Threading Technology‡ from Intel, a 2-way platform with dual-core processors will support up to 8 software threads; a 4-way platform up to 16 threads; an 8-way platform up to 32 threads; and a 16-way platform up to 64 threads. This will offer great flexibility for supporting multiple applications efficiently on a single platform.

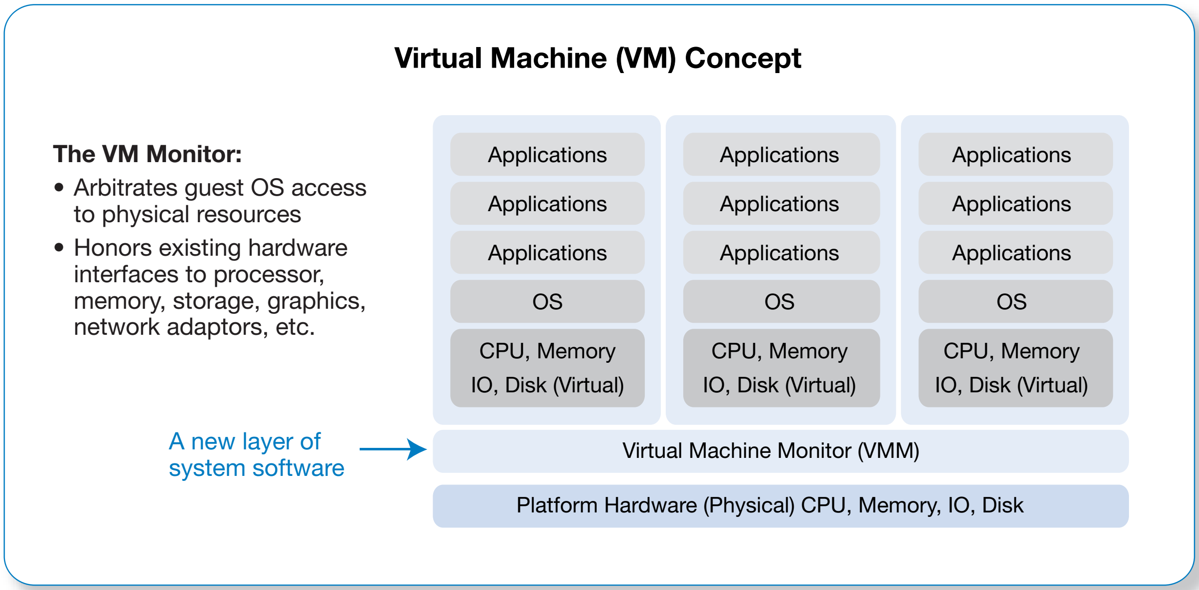
How It Works

To create virtual partitions in a server, a thin software layer called the Virtual Machine Monitor (VMM) runs directly on the server hardware. One or more guest OSs and application stacks can then be loaded on top of the VMM (Figure 3).

The VMM:

- **Emulates** a complete hardware environment—a virtual machine—for each software stack. Ideally, the OS and applications are completely unaware they are sharing hardware resources with other applications.
- **Isolates** execution in each virtual machine to support high security and availability.
- **Allocates** platform resources (processing, memory, I/O, storage, etc.) to optimize performance and align service levels with business requirements.
- **Encapsulates** software stacks (including the OS and state information), so they are easily copied and transferred to new virtual machines on the same or another platform.

Today's virtualization solutions perform all these functions. However, these software-only solutions often require complex workarounds. To enable better and more cost-effective virtualization with less software development effort, Intel has worked closely with industry-leading VMM vendors to define a new set of architectural standards. These standards are called Intel Virtualization Technology, and have already been released to help fuel faster innovation for virtualization solutions on Intel architecture-based enterprise platforms.



Virtual Machine (VM) Concept

The VM Monitor:

- Arbitrates guest OS access to physical resources
- Honors existing hardware interfaces to processor, memory, storage, graphics, network adaptors, etc.

Applications
Applications
Applications
OS
CPU, Memory IO, Disk (Virtual)
Applications
Applications
Applications
OS
CPU, Memory IO, Disk (Virtual)
Applications
Applications
Applications
OS
CPU, Memory IO, Disk (Virtual)
A new layer of system software
Virtual Machine Monitor (VMM)
Platform Hardware (Physical) CPU, Memory, IO, Disk

Figure 3. The key to server virtualization is the virtual machine monitor (VMM), a software application that manages hardware resources and arbitrates the requests of multiple operating systems and application stacks.

[8] For more information, visit the Intel Web site at http://www.intel.com/business/bss/products/server/consolidation/index.htm; or read the Intel white paper: *Twenty-to-One Consolidation on Intel® Architecture*, available at: http://cache-www.intel.com/cd/00/00/14/88/148803_148803.pdf.

Hardware-Assisted Virtualization for Next-Generation Solutions

> *"Intel's Vanderpool technology [now known as Intel Virtualization Technology] will make products such as VMware and Virtual PC more efficient, robust, secure and flexible."*
>
> – *Intel's Vanderpool Will Spark Virtualization Innovation*, Martin Reynolds, Gartner Research, January 21, 2005.

In a typical platform environment, there is a single operating system that controls platform resources, and arbitrates requests from one or more applications. In a virtualized platform environment, there may be many guest OSs running on top of the VMM software. To avoid conflicts, the VMM must maintain control of critical platform resources, and hand off limited control to each guest OS, as appropriate. The efficiency and integrity of these hand-offs are critical for optimal performance and reliability.

The Challenge

In current IA-32 architecture, all software runs in one of four "privilege levels" or "rings" (Ring-0 through Ring-3). The OS traditionally runs in Ring-0, which affords privileged access to the widest range of processor and platform resources. Individual applications usually run in Ring-3, which restricts certain functions (such as memory mapping) that might impact other applications. In this way, the OS retains control to ensure smooth operation.

Since the VMM must have privileged control of platform resources, the usual solution is to run the VMM in Ring-0, and guest OSs in Ring-1 or Ring-3. However, today's OSs have been specifically designed to run in Ring-0. This creates certain challenges. In particular, there are 17 "privileged" instructions that control critical platform resources. These instructions are used occasionally in most existing OS versions. When an OS is not running in Ring-0, any one of these instructions can create a conflict, causing either a system fault or a wrong response.

Software-Only Solutions

In general, there are two ways to deal with these 17 privileged instructions:

1. **Runtime Modification of the Guest OS**—In this case, the VMM monitors operation during runtime, and takes control of the processor whenever one of the 17 instructions arises in a guest OS. The VMM manages the conflict, then returns control to the guest OS.
2. **Static Modification of the Guest OS (Paravirtualization)**—In this case, the guest OS is modified prior to runtime.

Both these approaches have drawbacks. Runtime modification forces the VMM to provide complex workarounds during operation, which can impact performance. Paravirtualization prevents the VMM from hosting unmodified (legacy) guest OSs. Both approaches require extensive software development efforts from the VMM vendor, the OS vendor, or both. They also require that VMM and OS software be upgraded in tandem, which increases the cost and complexity of IT support.

Better Solutions with Intel® Virtualization Technology

Intel Virtualization Technology eliminates the gaps in current virtualization solutions by extending the core platform architecture. Enhancements include:

1. **A New, Higher Privilege Ring for the VMM**—This allows guest OSs and applications to run in the rings they were designed for, while ensuring the VMM has privileged control over platform resources. It eliminates many potential conflicts, simplifies VMM requirements, and improves compatibility with unmodified legacy OSs.
2. **Hardware-Based Transitions**—Handoffs between the VMM and guest OSs are supported in hardware. This reduces the need for complex, compute-intensive software transitions.
3. **Hardware-Based Memory Protection**—Processor state information is retained for the VMM and for each guest OS in dedicated address spaces. This helps to accelerate transitions and ensure the integrity of the process.

These enhancements will provide essential advantages, both for software vendors and IT organizations, including:

- **Reduced Cost and Risk for IT Organizations**—The independence of VMM and OS software will improve interoperability with unmodified legacy OSs. It will also help to eliminate the need to synchronize upgrades and patches in the datacenter. Support costs will be reduced, and IT organizations will be able to support a much wider range of OS versions on a consistent hardware and VMM platform.
- **Improved Reliability and Availability**—Reducing the size and complexity of the VMM, and making it independent of its guest OSs, reduces the potential for software conflicts that might otherwise slow or halt operations.
- **Enhanced Security**—Managing VMM transitions in hardware rather than software helps to strengthen the logical isolation of virtual partitions. The smaller and less complex VMM also provides fewer opportunities for software-based attacks.
- **Simpler VMM Development**—A key goal of Intel Virtualization Technology is to make VMM software independent of OS software. This will free VMM vendors from the resource-intensive task of adapting their code in response to OS patches and upgrades. It will also make it easier for existing solutions to take advantage of the latest platform capabilities, with less need for VMM development and tuning. Businesses can expect to benefit from faster time to market for new features and capabilities.

Ongoing Innovation

> *"…enterprises should understand the virtualization offerings and strategies of their server vendors, and make that a part of their server selection process."*
>
> – *Predicts 2004: Server Virtualization Evolves Rapidly,* T. Bittman, Gartner Research Note, November 14, 2003.

Intel is currently integrating Intel Virtualization Technology into all its server platforms.

- Support in Intel Itanium 2 processor-based systems is expected in the second half of 2005.
- Support in 64-bit Intel Xeon processor-based systems is expected in the first half of 2006.
- Intel is also accelerating integration into client platforms, with support expected in 2005 for desktops and 2006 for laptops (see the sidebar, *A New Era of PC Flexibility,* on page 5).

Intel Virtualization Technology is just the first step in a series of platform innovations that will provide increasing support for advanced virtualization solutions. Intel engineers are currently evaluating alternatives for I/O virtualization, which will make it easier for VMMs to manage and allocate I/O bandwidth among multiple applications running on the same hardware platform.

Intel also continues to work with leading VMM and OS developers (both third-party and open source), to provide a stronger foundation for their efforts and to ensure that next-generation advances target the most critical needs of business customers. In the years ahead, virtualization solutions on Intel architecture will continue to advance, providing IT organizations with increasingly powerful tools for consolidating applications, reducing their costs and optimizing business agility.

Intel Virtualization Technology is part of Intel's continuing drive to deliver a comprehensive set of market-leading platform technologies on industry-standard Intel-based servers. Examples of currently available technologies include Hyper-Threading Technology‡ (already discussed) and Intel® Extended Memory 64 Technology, which provides optimized support for both 32-bit and 64-bit applications on a single platform. Future innovations will include Intel® Active Management technology and LaGrande technology, which focus on platform management and security, respectively. In combination, these advanced platform capabilities will help IT organizations address some of their most critical challenges, and increase the business value of their IT investments.

Conclusion

> *"…over the next few years virtualization will redefine how we run enterprise infrastructure and give us a richer range of choices with which to create solutions."*
>
> – *Betting on Virtualization*, Mark Gibbs, Network World, November 15, 2004.

Virtualization represents the wave of the future for optimizing hardware utilization and datacenter agility. Intel architecture supports flexible and cost-effective virtualization solutions today, using software from VMware and Microsoft. These solutions are already delivering substantial value in a wide range of production environments.

Intel Virtualization Technology will increase these benefits, enabling Intel processor-based platforms to support virtualization in an integrated and seamless fashion. By providing a new privilege layer for VMM software, and supporting key virtualization functions in hardware, Intel Virtualization Technology will simplify VMM development and maintenance, improve interoperability with legacy OSs, enhance security and reliability, and reduce the cost and risk of implementation.

Intel Virtualization Technology is one of a series of platform advances that Intel will deliver over the next few years to provide critical support for enhanced datacenter flexibility, manageability, and security. Along with ongoing scaling of absolute performance and price/performance, these innovations will deliver increasing business value across the full range of Intel architecture-based servers.

For more information about Intel Virtualization Technology, visit the Intel Web site at: http://www.intel.com/technology/computing/vptech/.

‡ Hyper-Threading Technology requires a computer system with an Intel Pentium 4 processor at 3.06 GHz or higher, a chipset and BIOS that utilize this technology, and an operating system that includes optimizations for this technology. Performance will vary depending on the specific hardware and software you use. See http://www.intel.com/info/hyperthreading/ for information.