Technology Brief

Intel® Microarchitecture Nehalem
Virtualization Technology

Intel® Xeon® Processor

A Superior Hardware Platform for Server Virtualization

Improving Data Center Flexibility, Performance and TCO with the Intel® Xeon® Processor 5500 Series

Server virtualization is helping IT organizations improve data center productivity in fundamental ways. It lets you consolidate multiple operating systems and applications per physical server, reducing the size and costs of your IT infrastructure, while enabling you to deploy new applications in minutes. Virtualization also lets you move running applications from one server to another without downtime, for flexible workload management, high availability during planned maintenance or unplanned events. Investment in virtualization solutions is an intelligent business decision: the benefits in utilization, energy savings, manageability, service levels and cost models can be dramatic.

To gain full value of virtualization, you need servers that are built to handle the heavy and ever-changing demands of a virtualized and consolidated computing environment. To help you get maximum benefits from virtualization, Intel has built a better physical server platform with unique hardware-assist features to enhance the virtual data center. The Intel® Xeon® processor 5500Δ series is the first of this new generation of server platforms built with higher I/O bandwidth for higher virtualization performance plus multi-generation VM migration for unparalleled flexibility in virtualized environments. Next-generation Intel® Virtualization Technology◊ (Intel® VT) enhances native virtualization performance by up to 2.1x[1] and reduces roundtrip virtualization latency by up to 40 percent[2] with hardware-enhanced technologies built into Intel® processor, chipset, and network adapter.

"Choosing the right hardware platform for server virtualization is just as important as choosing the right virtualization software."[3]

– IDC

Processor: Intel® Virtualization Technology (Intel® VT-x)

- Intel® VT FlexMigration
- Intel® VT FlexPriority
- Intel® VT Extended Page Tables

Chipset: Intel® Virtualization Technology for Directed I/O (Intel® VT-d)

Network: Intel® Virtualization Technology for Connectivity (Intel® VT-c)

- Virtual Machine Device Queues (VMDq)
- Virtual Machine Direct Connect (VMDc)

Intel integrates hardware assists for virtualization into all key server components to help IT organizations consolidate more applications and heavier workloads on each server, and to improve flexibility, reliability, and TCO.

Superior Virtualization through Comprehensive Hardware Support

Servers of just a few years ago were designed to host a single operating system. Successful virtualization with these systems requires software that can emulate a complete hardware environment for every guest operating system. This is a compute-intensive process that introduces significant performance overhead. It can slow application response times, limit scalability, and create complexity that can impact reliability and security. Mixed server environments can also compromise the benefits of virtualization: as new servers are added, the inability to migrate VMs across different generations of servers limits data center flexibility.

Intel Virtualization Technology (Intel VT) addresses these challenges at the silicon level, by providing comprehensive hardware assists that boost virtualization software performance by up to 2.1x,[4] improve application response times and provide greater reliability, security and flexibility. These integrated hardware assists accelerate fundamental virtualization processes throughout the platform to reduce latencies and avoid potential bottlenecks. They also reduce the demands placed on the virtualization software, so more processor cycles are available for running business applications, and they enable VM migration across multiple generations of Intel® processor-based servers. As a result, you can consolidate more applications and heavier workloads per server to get better value from your server and software investments.

Intel works with VMware, Microsoft, Citrix, Parallels and many other virtualization software vendors to help ensure that Intel virtualization technologies are broadly supported in today's and tomorrow's solutions, so they deliver high value while being completely transparent to IT organizations and end-users. The functionality of your virtualization solutions is unchanged. Your virtual servers are simply more responsive, more scalable and more reliable.

The Processor: Intel® VT-x

Better Virtualization Support in Intel® Processors

Intel VT-x helps to improve the fundamental flexibility and robustness of software-based virtualization solutions. It reduces VMM interventions by eliminating the need for the VMM to listen, trap and execute certain instructions on behalf of the guest OS as is required in software-only virtualization. It also provides hardware support for transferring platform control between the VMM and guest OSs, so when VMM intervention is required, handoffs are faster, more reliable and more secure.

In addition, Intel VT-x has VM migration features that protect your IT investments and enhance flexibility for fail-over, load balancing, disaster recovery and maintenance:

- **Intel® VT FlexPriority:** When a processor is performing a task, it often receives requests or "interrupts" from other devices or applications that need attention. To minimize the impact on performance, a special register in the processor (the APIC Task Priority Register, or TPR) monitors the priority of tasks, so only interrupts that have a higher priority than the currently running task receive immediate attention. Intel FlexPriority creates a virtual copy of the TPR[5] which can be read, and in some cases, changed by guest OSs without VMM intervention. This can deliver major performance improvements for 32-bit OSs that make frequent use of the TPR.[6] (For example, it can improve performance by as much as 35 percent for applications running on Windows Server* 2000.[6])
- **Intel® VT FlexMigration:** One of the key benefits of virtualization is the ability to migrate running applications from one physical server to another without downtime. Intel VT FlexMigration is designed to enable seamless migrations among current and future Intel processor-based servers, even though newer systems may include enhanced instruction sets. With this technology, hypervisors can establish a consistent set of instructions across all servers in the migration pool, enabling seamless migration of workloads. The result is a more flexible and unified pool of server resources that functions seamlessly across multiple hardware generations.[7]

The Chipset: Intel® VT-d

Better Virtualization Support in Intel® Chipsets

As more guest OSs are consolidated per server, the movement of data into and out of the system (I/O traffic) increases and becomes more complex. Without hardware assistance, the VMM is directly involved in every I/O transaction. This not only slows down data movement, but also increases the load on server processors due to the higher VMM activity. It's as if every shopper in a busy shopping mall had to enter or exit the mall through a single door and get directions only from the mall manager. This would not only slow down customers, but would also prevent the manager from attending to other pressing issues.

Intel VT-d speeds data movement and eliminates much of the performance overhead by reducing the need for VMM involvement in managing I/O traffic. It accomplishes this by enabling the VMM to securely assign specific I/O devices to specific guest OSs. Each device is given a dedicated area in system memory that can be accessed only by the device and by its assigned guest OS.

Once the initial assignments are made, data can travel directly between a guest OS and its assigned devices. I/O traffic flows more quickly and the reduced VMM activity decreases the load on the server processors. Security and availability are also improved, since I/O data intended for a specific device or guest OS cannot be accessed by any other hardware or guest software component.

The Network: Intel® VT-c

Better Virtualization Support in Intel® I/O Devices

As businesses deploy more and more applications in virtualized environments, and as they take advantage of live migration to save power or boost availability, the demands on virtualized I/O increase significantly. Intel VT-c optimizes the network for virtualization by integrating extensive hardware assists into the I/O devices that are used to connect your servers to your data center network, storage infrastructure and other external devices. In essence, this collection of technologies functions much like a post office that sorts an

enormous variety of incoming letters, packages and envelopes and delivers them to their respective destinations. By performing these functions in dedicated network silicon, Intel VT-c speeds delivery and reduces the load on the VMM and server processors.

Intel VT-c includes two key technologies, which are now supported in all Intel® 10 Gigabit Server Adapters and selected Intel® Gigabit Server Adapters.

- **Maximize I/O Throughput with Virtual Machine Device Queues (VMDq):** In a traditional server virtualization environment, the VMM has to sort and deliver every individual data packet to its assigned virtual machine. This can consume a lot of processor cycles. With VMDq, this sorting function is performed by dedicated hardware in Intel Server Adapters. All the VMM has to do is route the presorted packet groups to the appropriate guest OSs. I/O latency is reduced and the processor has more cycles available for business applications. Intel VT-c can more than double I/O throughput and achieve near-native thoughput for virtualized applications, so more applications can be consolidated per server with fewer I/O bottlenecks.[8]

- **Improve Virtualization Performance with Virtual Machine Direct Connect (VMDc):** Virtual Machine Direct Connect (VMDc) allows virtual machines to access network I/O hardware directly, using the PCI-SIG Single Root I/O Virtualization (SR-IOV) standard, helping to improve virtualized performance dramatically. As discussed in the previous section, Intel VT-d enables a direct communication channel between a guest OS and an I/O port on the device. SR-IOV extends this by enabling multiple direct communication channels for each I/O port on the device. For example, each of ten guest OSs could be assigned a protected, dedicated 1 GB/s link to the corporate network through a single port on the Intel® 10 Gigabit Server Adapter. These direct communication links bypass the VMM switch to enable faster I/O performance with less load on the server processors.

A Better Platform for Virtualization

The Intel Xeon processor 5500 series is better physical platform for virtualization, with unique hardware-assist features to enhance the virtual data center and help tame server sprawl. The Intel Xeon processor 5500 series, built on Intel® Microarchitecture, codenamed Nehalem, expands the benefits of virtualization with innovations that boost performance, enhance I/O, and enable servers of different generations to be combined in the same virtualized server pool, facilitating application failover, load balancing, and disaster recovery capabilities.

These technologies are fully integrated, thoroughly tested and widely supported by leading virtualization software solutions. They provide IT organizations with a proven, industry-leading foundation for optimizing the value of their server and virtualization investments.

For the latest information about Intel Virtualization Technology, visit the Intel Web site at: www.intel.com/technology/virtualization/server

For detailed information about Intel VT-c and VT-d visit: www.intel.com/go/vtc

[Δ] Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor series, not across different processor sequences. See www.intel.com/products/processor_number for details.

[◊] Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM) and, for some uses, certain platform software enabled for it. Functionality, performance or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Please check with your application vendor.

[1] Performance results on VMmark benchmark. Xeon X5470 data based on published results. Xeon X5570 Intel internal measurement. (Feb 2009): HP Proliant ML370 G5 server platform with Intel Xeon processors X5470 3.33GHz, 2x6MB L2 cache, 1333MHz FSB, 48GB memory, VMware ESX V3.5.0 Update 3 Published at 9.15@7 tiles vs Intel® Xeon® processor X5570, 2.93 GHz, 8MB L3 cache, 6.4QPI, 72GB memory (18x4GB DDR3-800), VMware ESX Build 140815. Performance measured at 19.51@ 13 tiles.

[2] Source: Intel internal measurements. Intel® Xeon® processor 5500 series (Nehalem) vs. Intel® Xeon® processor 5400 series.

[3] Source: Choosing the Right Hardware for Server Virtualization, an IDC white paper sponsored by Intel, Doc # 211622, April 2008. http://www.intel.com/business/technologies/IDCchoosingvirthardware.pdf

[4] Performance results on VMmark benchmark. Xeon X5470 data based on published results. Xeon X5570 Intel internal measurement. (Feb 2009): HP Proliant ML370 G5 server platform with Intel Xeon processors X5470 3.33GHz, 2x6MB L2 cache, 1333MHz FSB, 48GB memory, VMware ESX V3.5.0 Update 3 Published at 9.15@7 tiles vs Intel® Xeon® processor X5570, 2.93 GHz, 8MB L3 cache, 6.4QPI, 72GB memory (18x4GB DDR3-800), VMware ESX Build 140815. Performance measured at 19.51@ 13 tiles.

[5] Intel® VT-x supports both 32-bit and 64-bit Intel® Xeon® processor-based solutions (Intel® 64 and IA-32).

[6] Intel tests demonstrate 35 percent performance gains for Windows Server* 2000 and 2003 SP1 versions running as guest operating systems.

[7] Intel® VT FlexMigration supports live VM migration across all Intel® Core™ microarchitecture-based servers and servers based on the new Intel microarchitecture (codenamed Nehalem). It is included in the new Intel® Xeon® processor 5500 series, and provides backward compatibility for live VM migration with current multi-core Intel® Core™ microarchitecture products and forward compatibility with future multi-core processors. Contact your preferred VMM vendor for support requirements.

[8] Results based on internal tests performed by Intel and VMware. For more information, see the Intelligent Queueing Technologies for Virtualization, An Intel-VMware perspective: Enhanced Performance in Virtualized Servers. http://download.intel.com/network/connectivity/products/whitepapers/Intel-VMware_VMDq_wp_May08.pdf

Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. Buyers should consult other sources of information to evaluate the performance of systems or components they are considering purchasing. For more information on performance tests and on the performance of Intel products, visit http://www.intel.com/performance/resources/ or call (U.S.) 1-800-628-8686 or 1-916-356-3104.

Relative performance is calculated by assigning a baseline value of 1.0 to one benchmark result, and then dividing the actual benchmark result for the baseline platform into each of the specific benchmark results of each of the other platforms, and assigning them a relative performance number that correlates with the performance improvements reported

Intel products are not intended for use in medical, life saving, life sustaining, critical control or safety systems, or in nuclear facility applications. All dates and products specified are for planning purposes only and are subject to change without notice

*Other names and brands may be claimed as the property of others.

Printed in USA 0309/HLW/OCG/XX/PDF Please Recycle 321597-001US