Technology Brief

Intel® Virtualization Technology

Intel® Xeon® Processor

A Superior Hardware Platform for Server Virtualization

Breakthrough Flexibility, Performance and TCO with the Latest Intel® Xeon® Processor-based Servers

"Choosing the right hardware platform for server virtualization is just as important as choosing the right virtualization software."
– IDC[1]

Server virtualization is helping IT organizations improve data center productivity in fundamental ways. It lets you consolidate your infrastructure to reduce costs, deploy new applications in minutes, and move running applications from one physical server to another without downtime for flexible workload management and cost-effective high availability and disaster recovery. The latest generation of Intel® Xeon® processor-based servers can help you maximize the benefits of virtualization. These servers deliver:

- **Industry-leading performance and energy-efficiency** so you can consolidate more applications and heavier workloads on each physical server, achieve faster application response times, and dramatically reduce space, power and cooling requirements in your data center. A number of recent innovations are particularly noteworthy in virtualized server environments. Intel® Hyper-Threading Technology† doubles the number of execution threads per core for more efficient processing of multiple workloads. Intel® Turbo Boost Technology§ delivers higher performance when you need it most by increasing processor frequency for peak workloads.

- **Broad server choice, from two-socket servers to scalable, mission-critical systems with up to 32 sockets.** A single four-socket server now provides up to 32 high-performance processor cores, 64 execution threads and a full terabyte of memory. This gives IT organizations tremendous capacity for consolidation with better performance than comparable competitive systems, even those with more cores. The latest Intel® Xeon® processor 7500 series also provides more than 20 new mainframe-inspired reliability, availability and serviceability (RAS) features so you can consolidate more applications with greater confidence.

- **Next-generation Intel® Virtualization Technology° (Intel® VT),** which provides comprehensive hardware assists for core virtualization functions across the entire server platform, including Intel® processors, chip-sets, and network adapters. Intel VT enhances virtualization performance by up to 3.7x[2] and supports live VM migration among multiple Intel Xeon processor-based server generations. It helps unleash the full potential of each server, so you get higher value from every new system you deploy.

Superior Virtualization through Comprehensive Hardware Support

Servers of just a few years ago were designed to host a single operating system, so virtualization software had to emulate a complete hardware environment for every guest operating system. This compute-intensive process introduces significant performance overhead that can slow application response times and limit scalability. It also introduces complexity that can impact reliability and security. Mixed server environments add to the challenge. Since virtual machines (VMs) cannot be migrated across different generations of these older servers, isolated virtualization pools can arise, which significantly limits data center flexibility.

Intel Virtualization Technology (Intel VT) addresses these challenges and more. It provides comprehensive hardware assists that:

- **Accelerate fundamental virtualization processes** to reduce latencies and avoid potential bottlenecks.
- **Reduce the demands placed on the virtualization software,** so more server resources (processor cycles, I/O bandwidth, etc.) are available for running business applications.
- **Enable live VM migration across multiple generations of Intel processor-based servers,** so business can maintain full data center flexibility as new servers are added.
- **Provide a hardware foundation for enhanced security** to protect systems, software, transactions and data more effectively against digital attacks.

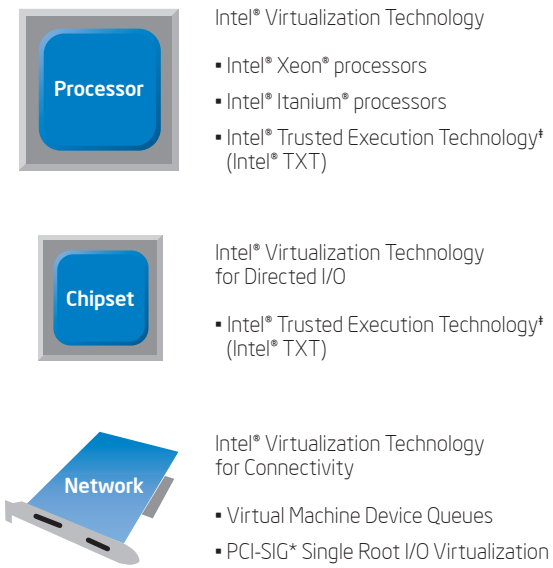

Figure 1. Intel integrates hardware assists for virtualization into all key server components to help IT organizations consolidate more applications and heavier workloads on each server, and to improve flexibility, reliability, and TCO.

The Processor: Intel® VT for IA-32 and Intel® 64Δ

Better Virtualization Support in Intel® Processors

In Intel processors, Intel VT helps to improve the fundamental flexibility, robustness and security of software-based virtualization solutions. It reduces the need for Virtual Machine Manager (VMM) interventions by eliminating the need for the VMM to listen, trap and execute certain instructions on behalf of each guest OS. When VMM interventions are required, it provides hardware support so handoffs between the VMM and guest OSs are faster, more reliable and more secure. Intel VT also provides hardware support for VM migration among multiple Intel Xeon processor generations, to support load balancing, fail-over, disaster recovery and downtime-free maintenance in multi-generation server environments.

- **Intel® VT FlexMigration:** Intel VT FlexMigration is designed to enable seamless migrations among current and future Intel Xeon processor-based servers by allowing hypervisors to establish a consistent set of instructions across all servers. This enables IT organizations to establish a more flexible, unified and expandable pool of virtualized server resources.[3]
- **Intel® VT FlexPriority:** When a processor is performing a task, it often receives requests or "interrupts" from other devices or applications. To minimize the impact on performance, a special register in the processor (the APIC Task Priority Register, or TPR) monitors the priority of tasks to prevent the interruption of one task by another with lower priority. Intel VT FlexPriority creates a virtual copy of the TPR[4] 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.[4]

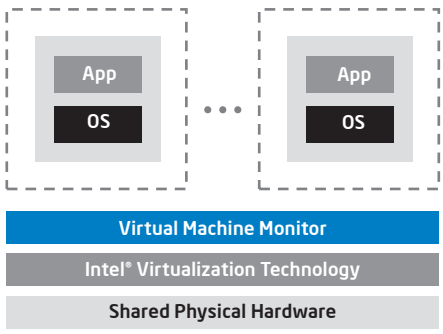

Figure 2. With Intel® VT-x, fewer VMM interventions are required and control can be passed between a guest OS and the VMM more quickly, reliably and securely.

- **Intel® Trusted Execution Technology:** Intel Trusted Execution Technology provides a hardware foundation for establishing trusted pools of virtualized servers, in which systems and software, including virtualization hypervisors, can only be launched into cryptographically verifiable "known good states." It offers fundamental advantages for safeguarding businesses against ever-growing threats, especially in today's virtualized data centers. It is currently supported in the Intel Xeon processor 5600 series designed for two-socket servers.[5]

The Chipset: Intel® VT for Directed I/O

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, which slows data movement and increases the load on server processors due to the increased VMM activity. It's as if every shopper in a busy 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 for Directed I/O speeds data movement by enabling the VMM to directly and securely assign specific I/O devices to specific guest OSs. Each device is given a dedicated area in system memory so data can travel directly and without VMM involvement. I/O traffic flows more quickly and there are more processor cycles available to run applications. 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 for Connectivity

Better Virtualization Support with Intel® Ethernet Server Adapters

High consolidation ratios and dynamic live VM migration increase the benefits of virtualization, but they also increase the demands on virtualized I/O. Intel VT for Connectivity optimizes the network for virtualization by integrating hardware assists into the devices that connect your servers to your unified data and storage network infrastructure. These technologies function much like a post office that sorts incoming letters, packages and envelopes. By sorting and routing data packets in the Intel Ethernet Controller, Intel VT for Connectivity speeds delivery and reduces the load on the VMM and server processors, enabling higher consolidation ratios, faster VM migration and more efficient sharing of I/O resources.

Intel VT for Connectivity includes two key technologies. Both are supported by select 10 Gigabit Intel® Ethernet Server Adapters and Gigabit Intel® Ethernet Server Adapters, which can be mixed and matched to address specific network requirements.

- **Virtual Machine Device Queues:** With Virtual Machine Device Queues, data packets are sorted in the Intel® Ethernet Controller, so I/O latency is reduced and server processors have more cycles available for business applications. This technology can more than double I/O throughput and provide near-native I/O performance, so more applications can be consolidated per server with fewer I/O bottlenecks.[6]
- **PCI-SIG* Single Root I/O Virtualization (SR-IOV):** SR-IOV is an industry-standard technology that allows multiple virtual machines to maintain direct communication channels with a single I/O device to improve I/O flexibility and utilization in virtualized environments. Intel's implementation supports and extends Intel VT for Directed I/O to provide near-native performance for each VM, with reduced load on the VMM and server processors. With this technology, a large number of VMs can each be assigned a protected, dedicated link to the network through a single port on a 10 Gigabit Intel® Ethernet Server Adapter.

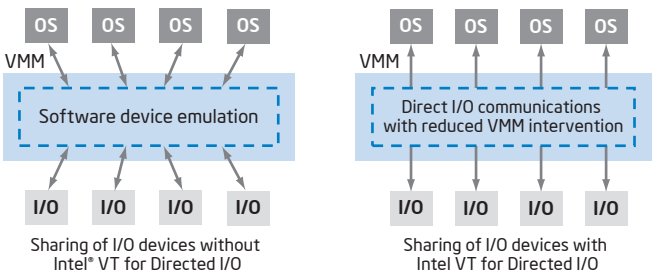

Figure 3. With Intel® VT for Directed I/O, the VMM can establish direct links between guest OSs and their assigned I/O devices, so traffic flows more quickly and there is less need for VMM intervention.

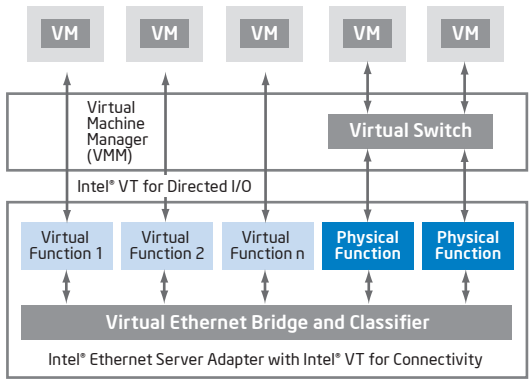

Figure 4. With integrated support for Intel® VT for Connectivity, Intel® Ethernet Server Adapters enable near-native I/O performance with flexible sharing of both physical ports and I/O bandwidth.

A Better Platform for Virtualization

Intel Xeon processor-based servers provide a superior hardware platform for virtualization. They deliver industry-leading performance and energy-efficiency across a wide range of server configurations, so you can consolidate more applications and heavier workloads per physical server. They also provide unique hardware-assist features that help boost application performance and I/O in virtualized environments, while improving data center flexibility through faster and more flexible VM migration.

Intel works closely with VMware, Microsoft, Citrix, Parallels, Oracle and many other virtualization software vendors to help ensure that these technologies are broadly supported and thoroughly tested, so your virtual servers are more responsive, scalable, reliable and secure across a wide range of scenarios. As you use virtualization to consolidate your infrastructure and improve service levels through dynamic workload balancing, high availability and disaster recovery, they can help you get better and more reliable value from every new server you deploy.

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

For detailed information about Intel VT for Connectivity and Intel VT for Directed I/O, visit www.intel.com/go/vtc

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.

† Hyper-Threading Technology requires a computer system with an Intel processor supporting Hyper-Threading Technology and an HT Technology enabled chipset, BIOS and operating system. Performance will vary depending on the specific hardware and software you use. See http://www.intel.com/info/hyperthreading/ for more information including details on which processors support HT Technology.

§ Intel® Turbo Boost Technology requires a platform with a processor with Intel Turbo Boost Technology capability. Intel Turbo Boost Technology performance varies depending on hardware, software and overall system configuration. Check with your platform manufacturer on whether your system delivers Intel Turbo Boost Technology. For more information, see http://www.intel.com/technology/turboboost.

◊ 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.

‡ Intel® Trusted Execution Technology is a security technology under development by Intel and requires for operation a computer system with Intel® Virtualization Technology, an Intel Trusted Execution Technology-enabled processor, chipset, BIOS, Authenticated Code Modules, and an Intel or other compatible measured virtual machine monitor. In addition, Intel Trusted Execution Technology requires the system to contain a TPMv1.2 as defined by the Trusted Computing Group and specific software for some uses. See http://www.intel.com/technology/security/ for more information.

Δ 64-bit computing on Intel architecture requires a computer system with a processor, chipset, BIOS, operating system, device drivers and applications enabled for Intel® 64 architecture. Processors will not operate (including 32-bit operation) without an Intel 64 architecture-enabled BIOS. Performance will vary depending on your hardware and software configurations. Consult with your system vendor for more information.

[1] IDC White Paper sponsored by Intel, Optimizing Hardware for x86 Server Virtualization, Doc # 219723, August 2009. http://www.intel.com/Assets/en_US/PDF/whitepaper/IDCchoosingvirthardware.pdf

[2] Claim: "Up to 3.7x more virtual machine performance than previous generations" Disclaimer: Intel comparison replacing one X7460 based server with one new X7560 processor based server. Consolidation Performance on VMmark* benchmark Comparison based on Intel internally measured as of 12 February 2010. 4S Intel® Xeon® processor X7460 based platform details IBM System x* 3850M2 server system with four Intel Xeon processors X7460 (16M cache, 2.66GHz, 6.4GT/s Intel QPI, 6C), 128GB (32x 4GB PC2-5300 667MHz Registered ECC DDR2 DIMMs, VMware ESX* 3.5.0 U3 GA. Referenced as published at 20.2 @ 14 tiles. For more information, see: http://www.vmware.com/files/pdf/vmmark/VMmark-IBM-2009-03-24-x3850M2.pdf. 4S Intel® Xeon® processor X7560 based platform details Intel® 7500 Chipset-based reference server platform with four Intel® Xeon® Processor X7560 (8-Core, 2.26 GHz, 24MB L3 cache, 6.4GT/s QPI), Intel EIST enabled, Turbo Boost enabled, Hyper-Threading enabled, NUMA enabled, Prefetchers enabled, 512GB (64x 8GB DDR3-1066) memory, VMware* ESX 4.0 Update 1 patch X, 2x Intel® 10 Gb CX4 Dual-Port Server Adapter, FC SAN 2x QLogic QLA2462, 16x 32GB SSD disk storage system. Source: Intel internal testing as of February 2010 referenced as estimated score of 75 @ 50 tiles.

[3] 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 multicore processors. Contact your preferred VMM vendor for support requirements.

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

[5] Two-socket servers are widely used as departmental and edge servers (Web servers, portal servers, email servers, etc.), which allows IT organizations to take advantage of these technologies in the kinds of servers that are common targets for digital attacks on the data center. Intel® TXT will also be integrated into future Intel Xeon processors designed for four-socket and larger systems. Intel TXT requires a server system with Intel® VT, an Intel TXT-enabled processor, chipset, Authenticated Code Module (ACM), enabled BIOS, and an Intel TXT-compatible MLE (OS or hypervisor). In addition, Intel TXT requires the system to contain a TPM v1.2, as defined by the Trusted Computing Group, and specific software for some uses.

[6] Results based on internal tests performed by Intel and VMware. Test Configuration: Ixia IxChariot* v7.0, 32 clients per port under test, High-performance throughput script, File size = 64-1K: 1,000,000 / 2K+:10,000,000 bytes (10GbE), Buffer sizes=64 Bytes to 64 KB, Data type – Zeroes, Data verification disabled, Nagles disabled. System under test: S5520HC, Intel Xeon processor X5570(8M Cache, 2.93 GHz, 6.40 GT/s Intel® QPI), 48GB DDR3 @ 1067 MHz, Intel® 5520 Chipset (Tylersburg), BIOS: S5500.86B.01.00.0038, VMware ESX 4.0. Clients: SuperMicro* 6015T-TV(twin), 2 Dual Core Intel Xeon processors 5160 @3.0GHz, 2 GB RAM, Intel® PRO/1000 PT Dual Port Server Adapter - v9.12.13.0 driver Windows* Server 2003 SP2 x64. Network Configuration: Cisco Catalyst* 6509, Clients connected @ 1 Gig Auto-neg.

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

Printed in USA 0310/SL/OCG/XX/PDF ♻ Please Recycle 323363-001US