Intel® Virtualization Technology
Processor Virtualization Extensions and Intel® Trusted execution Technology

Gideon Gerzon
Senior Processor Architect, Intel Mobile Group
Agenda

• Virtualization Basics
  • Emerging Usage Models
  • Virtualization Challenges

• The Intel Approach to Virtualization
  • Intel® Virtualization Technology & its Evolution

• Intel® VT Processor Extensions
  • Intel® VT FlexPriority
  • Intel® VT FlexMigration
  • Intel® VT Extended Page Tables
  • Intel® VT Virtual Processor ID

• Virtualization Performance Primer
  • The cost & The count of Overhead inducing factors

• The Intel Advantage

• Intel® Trusted Execution Technology (TXT)
## Today’s Virtualization Usage Models

<table>
<thead>
<tr>
<th>Static Server Consolidation</th>
</tr>
</thead>
<tbody>
<tr>
<td>End User Value</td>
</tr>
<tr>
<td>Reduce CapEx, increase utilization</td>
</tr>
</tbody>
</table>

**Beyond basic static consolidation, focus is on high availability and efficient resource allocation**
Virtualization
The Intel Connection

Realizing the promise of virtualization requires a multi-faceted approach

Hardware
- Intel architects processors, chipsets and communications components to support a complete virtualization solution

Software
- Intel’s SW Solutions Group aligns with key VMM & manageability vendors for optimized solutions on IA

The End User
- Understand the needs and constraints in IT virtualization and architect enhancements that enable those solutions
Intel® Virtualization Technology (Intel® VT) is a multi-generational roadmap of increasingly powerful enhancements to Intel Processors, Chipsets and I/O devices. It is a complementary technology to virtualization software products that enhances today’s virtualization solutions and lays foundation for future platform virtualization. Intel® VT provides hardware-assist to the virtualization software reducing its size and complexity enabling lower cost, more efficient, more powerful virtualization solutions.

Throughout this package:
VT-x refers to Intel® VT for IA-32 and Intel® 64
VT-i refers to the Intel® VT for Itanium® Architecture
VT-d refers to Intel® VT for Directed I/O
VT-c refers to Intel® VT for Connectivity
Intel® Virtualization Technology Evolution

Vector 3: IO Device Focus

Vector 2: Chipset Focus

Vector 1: Processor Focus

VMM Software Evolution

Software-only VMMs
Binary translation
Paravirtualization
Device emulations

Close basic processor “virtualization holes” in Intel® 64 & Itanium CPUs

 Richer/faster: Intel VT FlexPriority, FlexMigration EPT, VPID, ECRR, APIC-V

Richer IO-device functionality and IO resource sharing

• Assists for IO sharing:
  • PCI IOV captivated devs
  • VMDC
  • End-point translation caching
  • IO virtualization assists

Interrupt filtering & remapping
VT-DSI allows to track end-devs IOV

Core support for IO robustness & performance via DMA remapping

Perf improvements for interrupt intensive env, faster VM boot

All timeframes, dates, and products are subject to change without further notification

Copyright © 2007, Intel Corporation. All rights reserved.
CPU Virtualization with VT-x

New CPU Operating Mode
- VMX Root Operation (for VMM)
- Non-Root Operation (for Guest)
- Eliminates ring deprivileging

New Transitions
- VM entry to guest OS
- VM exit to VMM

VM Control Structure (VMCS)
- Configured by VMM software
- Specifies guest OS state
- Controls when VM exits occur (eliminates over and under exiting)
- Supports on-die CPU state caching

Guest OSes run at intended rings

Ring 3
- VM0
  - Apps

Ring 0
- VM Entry
  - WinXP
- VM Exit
  - Linux

VMX Root Mode
- VMM
  - Configuration
  - Memory and I/O Virtualization

H/W VM Control Structure (VMCS)
- VT-x
  - CPU0
  - CPUn

Processors with VT-x (or VT-i)
CPU Virtualization with VT-x

- Intel® Virtualization Technology present on Intel processors, enables a new privilege space where the VMM software can operate. It reduces the size and complexity of the VMM software improving its efficiency and enabling greater functionality.
  - Improves efficiency by reducing the need for VMM interventions with complex, compute intensive software translations
  - Enables greater functionality by allowing guest operating systems to run directly on the hardware avoiding the need to modify them
- Initially shipped in 2005 and now available across processor families from clients to servers.
Pre & Post Intel VT-x

- VMM de-privileges the guest OS into Ring 1, and takes up Ring 0
- OS un-aware it is not running in traditional ring 0 privilege
- Requires compute intensive SW translation to mitigate

- VMM has its own privileged level where it executes
- No need to de-privilege the guest OS
- OSes run directly on the hardware
Virtualization Performance Overhead

- Performance overheads arise from “exits” from guest OS to VMM
- Events that cause exits to VMM:
  1. Access to privileged CPU state
  2. Interrupt virtualization
  3. Page-table virtualization
  4. IO-device virtualization
- Each event has a cost:
  - CPU cycles to exit to and return from VMM
  - Time spent in event handler
  - Microarchitectural effects (TLB/Cache misses)
- Two ways to optimize performance:
  - Reducing event counts due to (1) - (4)
  - And/or, reducing event costs (e.g., transition times, handler costs)
Next-generation VT-x Features

1\textsuperscript{st} generation of Intel\textregistered VT shipped in 2005
- Several extensions to VT-x since that time...

On-going microarchitectural enhancements
- Reductions in VM entry/exit latencies
- No VMM software changes required

Architectural extensions
- VM Migration Support (FlexMigration)
- APIC Interrupt Virtualization Support (FlexPriority)
- Extended Page Tables (EPT)
- Virtual Processor IDs (VPID)
Latency Reductions by CPU Implementation

Intel® VT-x Transition Latencies by CPU

- Further improvements planned for future implementations

VMX Transition and Instruction Latency Improvements are dramatic and continuing

Measurements based on microbenchmark tests of VM entry / exit times on different Intel® VT implementations. Actual performance may vary (e.g., based on CPU freq).
Intel® Virtualization Technology
Processor Extensions

- Intel® VT FlexPriority
- Intel® VT FlexMigration
- Intel® VT Extended Page Tables
- Intel® VT Virtual Processor ID

Architectural enhancements geared to delivering
more powerful virtualization solutions
Background: APIC Architecture and Usage

- The Advanced Programmable Interrupt Controller (APIC)
  - A per-CPU interrupt controller with many control registers
  - Important register for this discussion: the task-priority register (TPR)
  - TPR used to mask interrupts based on priority of currently executing process

- TPR is accessed in two ways:
  - CR8 processor register (only available in 64-bit operating mode)
  - Memory-mapped register access

- Usage Patterns:
  - 64-bit OSes use CR8 to access
  - 32-bit OSes uses memory-mapped interface
  - Some OSes access the TPR with high frequency
Background: Virtualization of the APIC

• First generation Intel® VT provides support for CR8 virtualization

• With first generation Intel® VT, VMMs supporting use of memory-mapped TPR by guest OSes:
  - use binary patching or translation; avoids VMX transitions
  - disallow access to the TPR through active page tables, causing VM exit on access

• Significant performance and/or complexity issue without new hardware support...
Intel® VT FlexPriority
ON vs. OFF comparison using Virtual Iron 4.0.2 on vConsolidate

- Intel® VT FlexPriority improves VM access to Task Priority Register
  - Eliminates VMM intercepts of guest access to the TPR by enabling guests to access shadow register initialized by the VMM
- Feature Optimizes and accelerates interrupt virtualization on 32-bit guests
  - Up to 40% faster boot time with 32-bit Windows* XP guests
  - Up to 35% performance gain on guests running 32-bit Windows Server 2000 & 2003 SP1 versions
- Compares performance of Quad-Core Intel® Xeon® processor X7350 based server with Intel® VT FlexPriority ON & OFF configurations
  - Virtual Iron* 4.0.2 software
  - vConsolidate benchmark Beta 2
- Performance improvement enables efficient SMP configurations of 32-bit guest operating systems

Benefits of Intel® VT FlexPriority - Virtual Iron* 4.0.2 on vConsolidate

* All measurements conducted on platforms running 4xIntel® Xeon® Processor X7350, 32GB memory, vConsolidate ver 1.0, Virtual Iron 4.0.2 software, 1 CSU configuration, Sept 2007. Boot time improvement measured on Windows XP. vConsolidate measurement conducted by configuring the system with Windows 2000 SP4.
Intel® Virtualization Technology
Processor Extensions

- Intel® VT FlexPriority
- Intel® VT FlexMigration
- Intel® VT Extended Page Tables
- Intel® VT Virtual Processor ID

Architectural enhancements geared to delivering
more powerful virtualization solutions

Copyright © 2007, Intel Corporation. All rights reserved.
Intel® VT FlexMigration
Live Migration Challenges

• Live VM migration tools from any VMV require source and destination compatibility
• Applications may expect exact same behavior for machine instructions between the ‘To’ & ‘From’ platforms
  - Constraint exacerbated by innovation and introduction of new machine instructions
• Intel® VT FlexMigration allows VMM software to report the lowest common denominator of instructions set to the applications thereby broadening the live migration compatibility pool across generations of Intel processors

IT Investment Protection with Expanding Pools of Hardware Assisted Live VM Migration Compatibility
Intel® Virtualization Technology
Processor Extensions

- Intel® VT FlexPriority
- Intel® VT FlexMigration
- Intel® VT Extended Page Tables
- Intel® VT Virtual Processor ID

Architectural enhancements geared to delivering 
more powerful virtualization solutions
Extended Page Tables: Motivation

• VMM needs to retain control of physical-address space
  - With Intel® 64, paging is main mechanism for protecting that space
  - Intel® VT provides hooks for page-table virtualization...
  - ... but page-table virtualization in software is a major source of overhead

• Extended Page Tables (EPT)
  - A new CPU mechanism for remapping guest-physical memory references
  - Allows guest to retain control of legacy Intel® 64 paging
  - Reduces frequency of VM exits to VMM
EPT: Overview

- Guest can have full control over Intel® 64 page tables / events
  - CR3, CR0, CR4 paging bits, INVLPG, page fault
- VMM controls Extended Page Tables
- CPU uses both tables
- EPT (optionally) activated on VM entry
  - When EPT active, EPT base pointer (loaded on VM entry from VMCS) points to extended page tables
  - EPT deactivated on VM exit
EPT Translation: Details

- All guest-physical addresses go through extended page tables
  - Includes address in CR3, address in PDE, address in PTE, etc.
- Example given is for basic 32-bit paging
  - Also applies to other paging modes (e.g., PAE and Intel® 64)
- At leaf, Intel® 64 page faults recognized before EPT violations
EPT Performance

• Estimated EPT benefit is very dependent on workload
  - Typical benefit estimated up to 20\%\textsuperscript{1}
  - Outliers exist (e.g., forkwait, Cygwin gcc, > 40%)
  - Benefit increases with number of virtual CPUs (relative to MP page table virtualization algorithm)

• Secondary benefits of EPT:
  - No need for complex page table virtualization algorithm
  - Reduced memory footprint compared with shadow page-table algorithms
    ▪ Shadow page tables required for each guest user process
    ▪ Single EPT supports entire VM

EPT improves memory virtualization performance

\textsuperscript{1}Data derived from Intel internal simulation and modeling tools
Intel® Virtualization Technology
Processor Extensions

- Intel® VT FlexPriority
- Intel® VT FlexMigration
- Intel® VT Extended Page Tables
- Intel® VT Virtual Processor ID

Architectural enhancements geared to delivering
more powerful virtualization solutions
**VPID: Motivation**

- First generation of Intel® VT forces flush of Translation Lookaside Buffer (TLB) on each VMX transition

- Performance loss on all VM exits

- Performance loss on most VM entries
  - Most of the time, the VMM has not modified the guest page tables and does not require TLB flushing to occur
  - Exceptions include emulating MOV CR3, MOV CR4, INVLPG
  - Better VMM software control of TLB flushes is beneficial
VPID: New Support for Software Control of TLB

• VPID activated if new "enable VPID" control bit is set in VMCS

• New 16-bit virtual-processor-ID field (VPID) field in VMCS
  - VMM allocates unique value for each guest OS
  - VMM uses VPID of 0x0000, no guest can have this VPID

• Cached linear translations are tagged with VPID value

• No flush of TLBs on VM entry or VM exit if VPID active
VPID Performance

- VPID benefit is very dependent on workload and memory virtualization mechanism

- Without EPT:
  - Most stressful of CPU-intensive workloads (e.g., gzip) show only small improvements with VPID
  - Process and memory-intensive workloads gain an estimated 1.5% - 2%\(^1\)
  - Worst-case synthetic benchmarks gain an estimated 3%-4%\(^1\)

- With EPT:
  - VM-exit frequency decreases but the cost of TLB fills increases
  - VPIIDs required to make EPT effective under stressful loads
  - For process/memory-intensive workloads gain an estimated >2%\(^1\)
  - Worst-case synthetic benchmarks gain an estimated 10%-15%\(^1\)

\(^1\)Data derived from Intel internal simulation and modeling tools

VPID improves TLB performance with small VMM development effort

Copyright © 2007, Intel Corporation. All rights reserved.
VT-d Overview

VT-d is platform infrastructure for I/O virtualization
- Defines an architecture for DMA and interrupt remapping
- Implemented as part of core logic chipset
- Will be supported broadly in Intel server and client chipsets
Intel VT for Directed I/O - Protection: Reliability & Security thru device isolation

Virtual Machines

Virtual Machine Monitor (VMM)

IO Devices

Phys Mem

Device Driver

Hardware DMA Remap Mechanisms under VMM Control

Copyright © 2007, Intel Corporation. All rights reserved.
Remapping Benefits for Native OS, VMM

1. Protection:
   - Enhance security and reliability through device isolation
   - End to end isolation from VM to devices

2. Performance:
   - Allows I/O devices to be directly assigned to specific virtual machines
   - Eliminate Bounce buffer conditions with 32-bit devices

3. Efficiency:
   - Interrupt isolation and load balancing
   - System scalability with extended xAPIC support

4. Core platform infrastructure for Single Root IOV
VT Summary

- Virtualization implementations extend beyond basic static server consolidation, focus is on high availability and efficient resource allocation
- Intel offers Intel® Virtualization Technology with processor, chipset and IO ingredients that enhance today’s virtualization solutions and lays foundation for future platform virtualization that enable new usage models
- Today’s virtualization solutions benefit from Intel® VT through extended capabilities and improved efficiency. These solutions will further benefit from continuous improvements yet to come—improvements that will optimize and accelerate virtualization solutions on Intel Architecture
- Overall Platform Performance Matters. This comes from micro-architectural improvements (e.g. Intel® Core™) and architectural improvements (e.g. Intel® I/OAT, VMDq)
- Intel has a solid roadmap for processor innovation as well as virtualization architectural enhancements that are geared to delivering more powerful virtualization solutions with near native performance
Intel Advantage in virtualization

**Quad-Core (Processor)**
Unrivaled energy efficient native performance

**Intel® VT-x / VT-i (Processor)**
Hardware assists for robust and simpler virtualization

**Intel® VT FlexPriority** - Interrupt Acceleration

**Intel® VT FlexMigration** - Flexible live Migration

**Intel® VT for Directed I/O (Chipset)**
Reliability and Security through device Isolation
I/O performance with direct assignment

**Intel® VT for Connectivity (Device)**
NIC Enhancement with VMDq
Single Root IOV Support
Network Performance and reduced CPU utilization

**Intel® I/OAT for virtualization**
Lower CPU Overhead and Data Acceleration

**IOV PCI-SIG* Participation**
Intel® Trusted Execution Technology (TXT)

Technical Overview

- Domain isolation
- **MLE Identity**
  - OS or VMM
- DMA protection
- Control of configuration

Measured Launched Environment (MLE)

Hardware

CPU

TPM

Chipset
Hardware command, GETSEC [SENTER], provides synchronization, special bus cycles, and a special environment for performing the MLE measurement.

Hardware validates the software that is capable of validating platform configuration and performing the MLE measurement.

After validation the software performs the platform validation and MLE measurement.
Load SINIT and MLE into memory
1. Invoke GETSEC [SENTER]
2. Establish special environment
3. Load SINIT into ACEA
4. Validate SINIT digital signature
5. Store SINIT identity in TPM
6. SINIT measures MLE in memory
7. Store MLE identity in TPM
8. SINIT passes control to MLE
Platform Security Technologies

Business Client PC

User

Trusted

Apps

OS/Service

Hypervisor

CPU

BIOS

MCH/ICH

TPM

Memory

Peripherals

Network

IT Console

Platform Technologies

Verified Client Launch (TXT)

Client Virtualization (VT/VT-d)

Agent S/W Presence

Remote IT Security

PC System Defense

Encryption (AES-NI)

Data Encryption (Danbury)

Trusted Platform Module (TPM)
Additional information sources:

• For specifications and to learn more
  - Intel® VT Web Site:
  - Intel Virtualization Software Community:
    - [http://www.intel.com/software/virtualization](http://www.intel.com/software/virtualization)
  - Intel® Trusted Execution Technology (TXT)
    - [http://www.intel.com/security](http://www.intel.com/security)
    - [http://www.microsoft.com/security](http://www.microsoft.com/security)
Risk Factors

This presentation contains forward-looking statements. All statements made that are not historical facts are subject to a number of risks and uncertainties, and actual results may differ materially. Please refer to our most recent Earnings Release and our most recent Form 10-Q or 10-K filing available on our website for more information on the risk factors that could cause actual results to differ.
Legal Disclaimer

• INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL’S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL® PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. INTEL PRODUCTS ARE NOT INTENDED FOR USE IN MEDICAL, LIFE SAVING, OR LIFE SUSTAINING APPLICATIONS.

• Intel may make changes to specifications and product descriptions at any time, without notice.

• All products, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice.

• Intel, processors, chipsets, and desktop boards may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are 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.

• Intel, Intel Inside, Merom, Penryn, Nehalem, Dunnington, Harpertown, Yorkfield and the Intel logo are trademarks of Intel Corporation in the United States and other countries.

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

• Copyright © 2007 Intel Corporation.
Backup Foils
Without hardware support

What the VMM Does ...
- Emulates a complete hardware environment for every Virtual Machine
- Allocates platform resources
- Isolates execution in each virtual machine

Virtualization solutions without hardware support work, but there are limitations and require frequent software intervention
Software-Only Virtualization

Summary of Challenges

Complexity
- CPU “virtualization holes” require binary translation or paravirtualization
- Must emulate IO devices in software

Performance
- Overheads of excessive or “spurious” faulting
- Overheads of page-table virtualization
- Extra memory required (e.g., translated code, shadow page tables)
- IO requests must traverse two IO stacks (first guest OS, then host OS)

Functionality
- Paravirtualization may limit supported guest OSes
- Guest OSes “see” only simulated platform and IO devices

Reliability and Protection
- IO device drivers run as part of host OS or hypervisor
- No protection from errant DMA that corrupts memory
Intel® VT FlexPriority: APIC TPR Virtualization Support

• Intel® FlexPriority adds support for virtualization of memory-mapped TPR

• CPU maintains a “virtual TPR” register in memory

• On guest read of memory-mapped TPR:
  - CPU returns shadow value from virtual TPR

• On guest write to memory-mapped TPR:
  - CPU writes value to virtual TPR and VM exits only if written value is under threshold
Maximize Virtualization Flexibility
VMware* & Intel® VT FlexMigration Assist

Starting with Quad-Core Intel® Xeon® based processors\(^1\), Intel has architected existing and future products to allow hardware compatibility to support live VM migration across multiple generations of Intel processor families. Intel has enabled industry leading software vendors to take full advantage of this new capability for advanced virtualization usages.

Jointly innovating
to enable more flexible live virtual machine migration across multiple generations of Intel® processors

All timeframes, dates, and products are subject to change without further notification

\(^1\)Backward compatibility for live VM migration also exists with current dual-core Intel® Core™ microarchitecture products (Intel Xeon 5100 and Intel Xeon 3000) and forward compatibility with future dual and multi-core processors. Contact your preferred VMM vendor for support requirements.

Copyright © 2007, Intel Corporation. All rights reserved.
Physical Address Translation

Guest Physical Address

EPT Base Pointer

Extended Page Table Entry (EPTE) format described next…
Intel® VT Extended Page Tables

- Optimizes and accelerates memory virtualization by enabling Guest OS to modify its own page tables
  - Eliminates VM exits resulting on performance gains
  - Reduces Shadow Page Tables required for each guest user process delivering memory savings

- CPU TLB ‘walks’ Virtual memory to Physical memory
- EPT ‘walks’ Physical memory to Machine memory
VPID: Usage

• Legacy VMMs will not use VPID
  - VMX transitions flush TLBs, supporting old usages

• New VMMs can use VPID field
  - Retains linear mappings across VMX transitions

• Use of INVVPID instruction
  - Issued by VMM when it has modified page tables for a guest
    • E.g., as part of a shadow page-table virtualization algorithm
  - Not expected to be used if EPT is active
**Intel® VT Virtual Processor ID**

- Optimizes **VM** transition time by avoiding unconditional flushes of cached structures
  - Translation from Virtual to Physical addresses are maintained in CPU cache
  - Ability to assign a VM ID to tag CPU hardware structures (e.g. TLBs)
  - Avoid unconditional flush of data between on VM transitions

- **CPU** is aware of what data belongs to each VM
- TLB data is tagged and maintained between VM Exits
Intel® VT-x Extensions (review)

**Intel® Virtualization Technology FlexPriority**
- Architectural enhancement that delivers performance gain in virtualization by accelerating virtualization of interrupts on 32-bit guests
- Feature eliminates VMM intercepts of guest access to the Task Priority Register by enabling guests to access shadow register initialized by the VMM

**Intel® Virtualization Technology FlexMigration**
- Architectural enhancement to ease VM Migration constraints across generations of Intel processors
- Delivers investment protection and maximizes migration flexibility to enable zero downtime server maintenance that supports disaster recovery, load balancing, fail over, and more

**Intel® VT Extended Page Tables**
- Hardware assist for page table virtualization to reduce virtualization overhead
- Eliminates VM exits to the VMM for shadow page-table maintenance

**Intel® VT Virtual Processor ID**
- Ability to assign a VM ID to tag CPU hardware structures (e.g. TLBs)
- Avoid unconditional flushes on VM transitions to give a lower-cost VM transition time

*Focused on maximizing migration flexibility as well as optimizing, accelerating, and improving efficiency of virtualization software.*
Virtualization Performance
Robust Tick Tock Roadmap

Roadmap will continue to deliver higher raw performance (Moore’s Law), and architectural enhancements to improve efficiency in virtualized environments.

All timeframes, dates, and products are subject to change without further notification.

Copyright © 2007, Intel Corporation. All rights reserved.
Putting the Pieces Together

• Build on existing Intel platform features

• Simplified deployability
  - How do you get underlying security SW provisioned?

• Flexible security
  - How to provide protections for SW that runs in the User’s OS?

• “No excuses” performance
  - How do you avoid the security/performance trade off?
Virtualization Overhead
Optimization & Acceleration Improvements

Improvements focused on optimization & acceleration

Algorithm Optimizations to Intel® VT-x:
Intel is working with VMM vendors to tune their binary translator algorithms to work better with Intel® VT-x.

Virtualization SW Overhead:
Intel® VT architectural enhancement that allows guest OS to program page tables without VMM intervention

Others:
Additional microarchitectural and architectural enhancements in the works further mitigate virtualization software overhead

Intel working to deliver near native performance by reducing event count as well as event costs

Results have been simulated and are provided for informational purposes only. Results were derived using simulations run on an architecture simulator. Any difference in system hardware or software design or configuration may affect actual performance.