Westmere Xeon-56xx "Tick" CPU

Dave Hill Westmere Architecture

Muntaquim Chowdhury Westmere Design

Intel Oregon

Legal Disclaimer

- INFORMATION IN THIS DOCUMENT IS PROVIDEDIN 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 available on request.
- Nehalem, Merom, Boxboro, Millbrook, Penryn, Westmere, Sandy Bridge and other code names featured are used internally within Intel to identify products that are in development and not yet publicly announced for release. Customers, licensees and other third parties are not authorized by Intel to use code names in advertising, promotion or marketing of any product or services and any such use of Intel's internal code names is at the sole risk of the user
- 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, Intel Core, Intel Xeon, Intel Core2 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.
-

Legal Disclaimers

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/benchmark_limitations.htm or call (U.S.) 1-800-628-8686 or 1-916-356-3104.

Intel does not control or audit the design or implementation of third party benchmarks or Web sites referenced in this document. Intel encourages all of its customers to visit the referenced Web sites or others where similar performance benchmarks are reported and confirm whether the referenced benchmarks are accurate and reflect performance of systems available for purchase.

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.

SPEC, SPECint, SPECfp, SPECrate. SPECpower, SPECjAppServer, SPECjbb, SPECjvm, SPECWeb, SPECompM, SPECompL, SPEC MPI, SPECjEnterprise* are trademarks of the Standard Performance Evaluation Corporation. See http://www.spec.org for more information. TPC-C, TPC-H, TPC-E are trademarks of the Transaction Processing Council. See http://www.tpc.org for more information.

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.

Hyper-Threading Technology requires a computer system with a processor supporting HT Technology and an HT Technology-enabled chipset, BIOS and operating system. Performance will vary depending on the specific hardware and software you use. For more information including details on which processors support HT Technology, see here

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 ”

No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer system with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). The MLE could consist of a virtual machine monitor, an OS or an application. 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. For more information, see here

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

Risk Factors

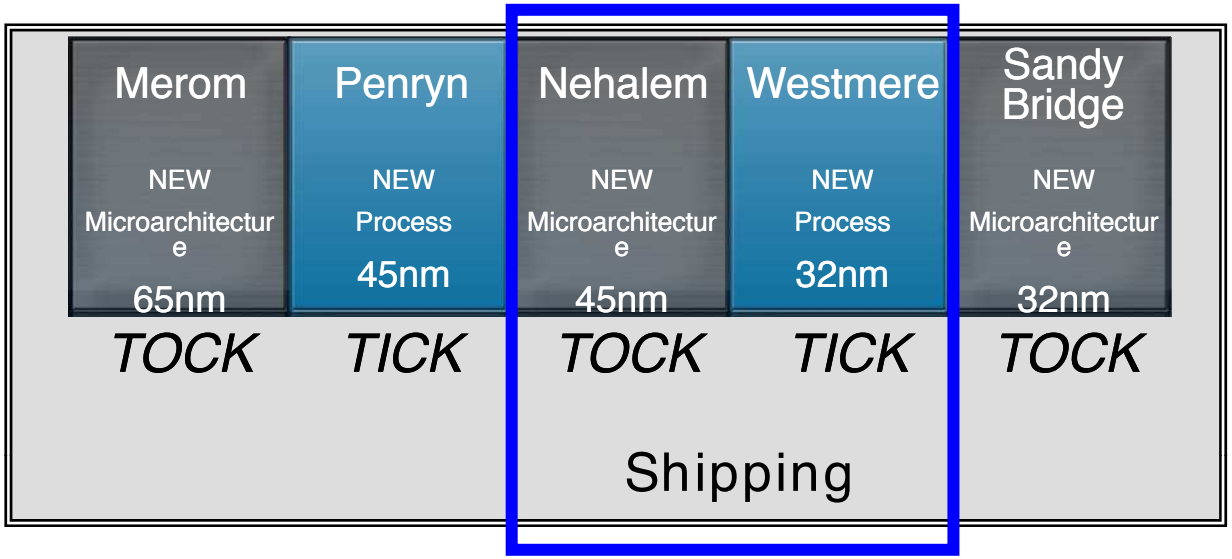
This presentation contains forward-looking statements that involve a number of risks and uncertainties. These statements do not reflect the potential impact of any mergers, acquisitions, divestitures, investments or other similar transactions that may be completed in the future. The information presented is accurate only as of today's date and will not be updated. In addition to any factors discussed in the presentation, the important factors that could cause actual results to differ materially include the following: Demand could be different from Intel's expectations due to factors including changes in business and economic conditions, including conditions in the credit market that could affect consumer confidence; customer acceptance of Intel's and competitors' products; changes in customer order patterns, including order cancellations; and changes in the level of inventory at customers. Intel's results could be affected by the timing of closing of acquisitions and divestitures. Intel operates in intensely competitive industries that are characterized by a high percentage of costs that are fixed or difficult to reduce in the short term and product demand that is highly variable and difficult to forecast. Revenue and the gross margin percentage are affected by the timing of new Intel product introductions and the demand for and market acceptance of Intel's products; actions taken by Intel's competitors, including product offerings and introductions, marketing programs and pricing pressures and Intel's response to such actions; Intel's ability to respond quickly to technological developments and to incorporate new features into its products; and the availability of sufficient supply of components from suppliers to meet demand. The gross margin percentage could vary significantly from expectations based on changes in revenue levels; product mix and pricing; capacity utilization; variations in inventory valuation, including variations related to the timing of qualifying products for sale; excess or obsolete inventory; manufacturing yields; changes in unit costs; impairments of long-lived assets, including manufacturing, assembly/test and intangible assets; and the timing and execution of the manufacturing ramp and associated costs, including start-up costs. Expenses, particularly certain marketing and compensation expenses, vary depending on the level of demand for Intel's products, the level of revenue and profits, and impairments of long-lived assets. Intel is in the midst of a structure and efficiency program that is resulting in several actions that could have an impact on expected expense levels and gross margin. Intel's results could be impacted by adverse economic, social, political and physical/infrastructure conditions in the countries in which Intel, its customers or its suppliers operate, including military conflict and other security risks, natural disasters, infrastructure disruptions, health concerns and fluctuations in currency exchange rates. Intel's results could be affected by adverse effects associated with product defects and errata (deviations from published specifications), and by litigation or regulatory matters involving intellectual property, stockholder, consumer, antitrust and other issues, such as the litigation and regulatory matters described in Intel's SEC reports. A detailed discussion of these and other factors that could affect Intel's results is included in Intel's SEC filings, including the report on Form 10-Q for the quarter ended June 27, 2009.

Agenda

- The "Tick" Challenge at Intel
- Westmere Xeon-56xx (EP) : 1000 Foot View
- Xeon-56xx Architectural Focus areas :
  - Performance Scalability
  - Virtualization
  - Security
  - Power-Efficiency

Note : Westmere Xeon-56xx presentation material today, performance measurement data, and described product SKU's are based on shipping products.

Intel Tick-Tock background



- "Tock-Tick" Pairs tightly coupled leverage of oneanother
- Tocks introduce major platform changes and architectural themes
  - on a mature process
- Ticks introduce the new Process capabilities
  - advancing a mature Tock architecture

WSM-56xx Design Challenges

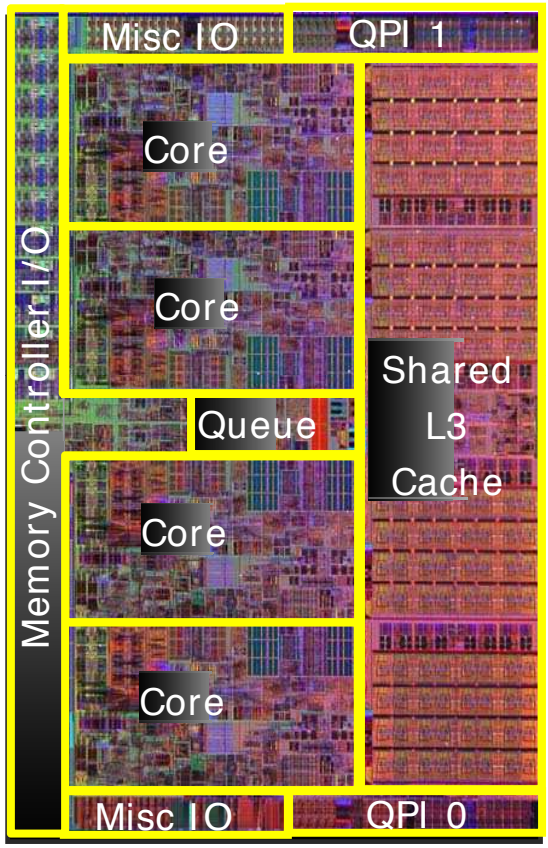
Ticks are developed in a constrained environment

- Timeline: Shorter design cycle based on TTM (don't holdup FAB)
- Process Stability: New process means Design Development is concurrent with Process fine-tuning. On the fly adjustments.
  - Example : moving tock design to new process creates some different speedpaths, circuits that behave differently than last process. Risk of new tick process at beginning of life being slower than the more mature tock process. Takes back-forth work between Design, Process, Arch to find balance.
- Design Data-Base Leverage from Tock :
  - Maximize Leverage of existing Design database inherited from tock
    - Typical reuse goal of at least 60% of tock RTL. WSM was a little higher.
  - Reuse available at transistor/layout level, not just RTL & tests
  - Innovations have to be non-disruptive to the inherited DB, form-factor
  - Not just an Intel thing.. All OEM re-validation risk and effort benefits from leveraging as much as possible in a "drop in" approach to the tick.

Challenge: Deliver Compelling Goodness despite constraints

Westmere 56xx – What is it ?

263mm

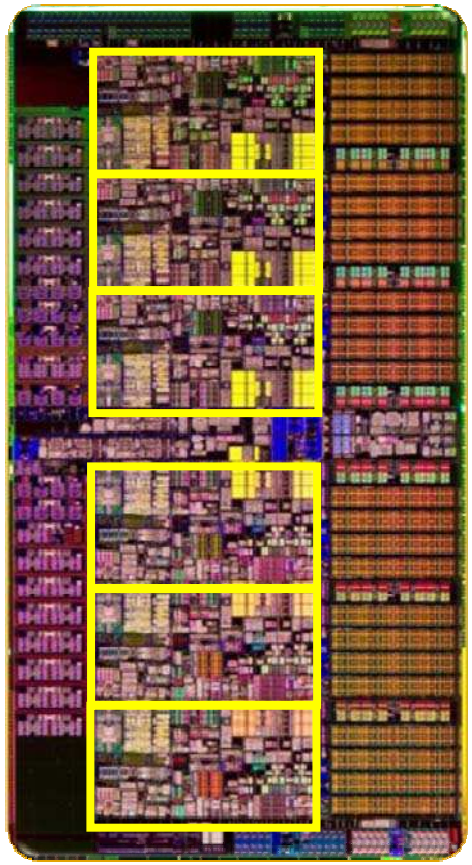


45nm Nehalem (55xx series)

- 32nm ~drop-in compatible to NHM 55xx spec compliant UP and DP platforms. 1366 pins (600+ Power/Vss) socket-B same as NHM.
- Conceptually simple :
- +50% cores (6)
- +50% L3 cache(12MB)
- -10% area (239mm)
- similar total power and thermal characteristics to four core NHM it replaces

Converged Core Architecture

239mm



32nm Westmere (56xx series)

WSM-56xx Focus Areas

- Platform Compatible. Straightforward Scalability
  - Leverage 32nm process to grow Core-Count, L3 Cache 50%
  - Ease new product transition pain and risk for customers.
- Power Performance
  - Leverage 32nm process as more performance at similar power envelope, **OR** similar performance at lower power levels.
- Security
  - A step forward. HW assist AES Encrypt/Decrypt. TXT extensions
- Virtualization
  - Key Datacenter ask : Boost Virtualization performance
- Over 100 additional incremental improvements
  - Customer feedback requests and incremental improvements from tock learnings fill out net team execution bandwidth available (top-10 next page)

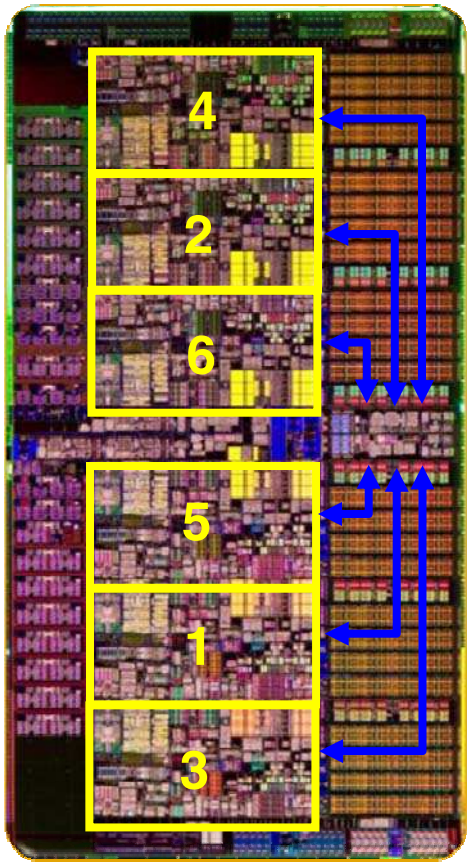
Westmere 56xx – Top 10 Improvements

- Added 50% cores, 50% L3 cache- within NHM platform constraints.
- Memory Support
  - 1.5v DDR3, plus new LV-DDR3 support (1.35v for better platform power)
  - 2 DIMM per channel @ 1333 DDR3 (NHM 2DPC support up to 1067)
- More peak CPU and I/O Bandwidth to memory
  - 64 ➔ 88 uncore buffer depth increase per socket for supporting more transactions to DDR in flight.
- AES-NI – 7 new instructions
  - Benefits encrypt / decrypt standard used for securing web and storage information
- TXT (trusted execution)
  - Measured Launch Environment to harden platforms from hypervisor, bios, rootkit attacks.
- Improved Virtualization
  - Real-mode support, Lower transition latencies vs NHM
- 1 GBpage table entries
  - Support for larger page size (for multi GByte High Performance Computing memory footprints)
- PCID
  - Tag TLB entries with process context ID so they may persist across CR3 writes
  - Similar to VPID functionality added in NHM, but in non-Virtualized format
- Two more MTRR's (10 variable memory type range registers)
  - Overdue help for BIOS code setup of memory type regions
- Always running Apic Timer
  - resolves prior art documented apic-timer drift/timewarp issue during power modes where core was off.

Performance Scalability

How it was done, and Results

How was it done ?



32nm Westmere (56xx series)

- Pre-plumb NHM platforms for 32nm
  - example : 32nm uses slightly different Core, UnCore and I/O voltages than 45nm. NHM spec'ed the voltage regulators, voltage range selection interface and current requirements to cover 45nm, and 32nm Westmere needs.
- Architect NHM with Uncore, QPI, DDR headroom
  - Cache tag bandwidth, IDI, PCU, QPI built to survive tick scaling needs.
- Upfront work w/Manufacturing to tune process
  - Lots of work getting transistor characteristics, cell library, metal pitch, etc to enable best transition of tock design to the new tick process.
- Core team builds 32nm WSM core database (AES etc)
- UnCore team extends buffered cross-bar to 6-core plumbing
  - Slide 4-cores away from Uncore
  - Insert cores 5,6 & add core-uncore IDI domain-jump connections
  - Find and extend many 2-bit fields to 3 bits
- Extend to 12MB L3 cache, XSnp-filters, PCU to 6core, schedulers, etc
  - L3 still 16-way shared. SET address arithmetic changed.
- Add a clock each direction to IDI,L3$, QPI, DDR paths for increased effective physical distances involved (simple RC issue).
- Repartition and bolster buffering.
  - Bumped 64→88 max DDR requests per socket.
- Resolve and validate the many details
- Backend work w/Manufacturing to tune process and sorting
  - Attain freq and power characteristic goals of the "drop in" paradigm.
  - Parts are sorted and fused at test time to best voltage and frequency bins.
  - Above is key... no one voltage at which WSM parts run

Scaling Results : Xeon® 5500 → Xeon® 56xx

Left-Side = 4Core Nehalem 55xx Parts
Right-Side = Westmere 56xx Parts

Usage	Xeon® 5500		Xeon® 56xx	
Advanced • 6.4 GT/s QPI • 8MB / 12MB • DDR3 1333 • Turbo Boost • HT	X5570 2.93 GHz 95W X5560 2.80 GHz 95W X5550 2.66 GHz 95W	**Maximum Performance** 6 Cores or 4 Cores (freq optimized)	X5680 6C 3.33 GHz 130W X5670 6C 2.93 GHz 95W X5660 6C 2.80 GHz 95W X5650 6C 2.66 GHz 95W	X5677 4C 3.46 GHz 130W X5667 4C 3.06 GHz 95W L5640 6C 2.26 GHz 60W
Standard • 5.86 GT/s QPI • 8MB / 12MB • DDR3 1066 • Turbo Boost • HT	E5540 2.53 GHz 80W E5530 2.40 GHz 80W E5520 2.26 GHz 80W	**Best Price Performance** Higher Freq More Cache	E5640 4C 2.66 GHz 80W E5630 4C 2.53 GHz 80W E5620 4C 2.40 GHz 80W	L5630 4C 2.13 GHz 40W L5609 4C 1.86 GHz 40W
Basic • 4.8 GT/s QPI • 4M cache • DDR3 800	E5506 2.13 GHz 80W E5504 2.00 GHz 80W E5502 1.86 (2C) 80W	**Cost-Optimized** Higher Frequency Xeon® E5500 SKUs	E5507 2.26 GHz (4C) 80W E5506 2.13GHz (4C) 80W E5503 2.00 GHz (2C) 80W	

Freq-Optimized

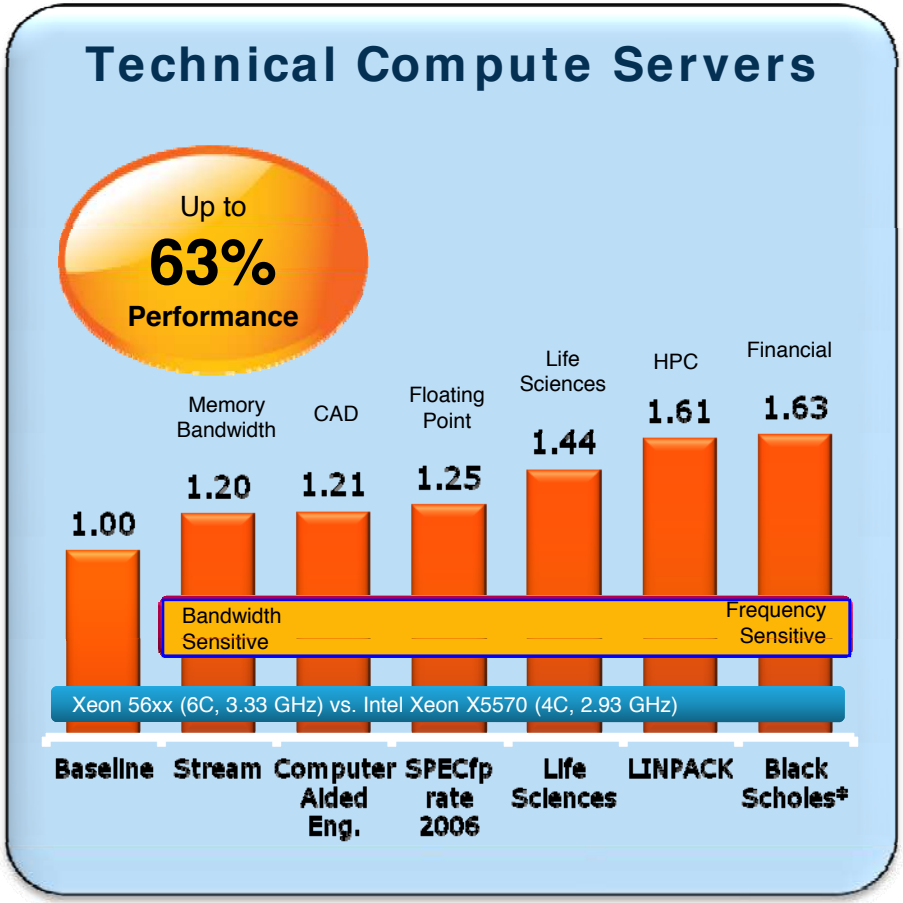
Low Power Options

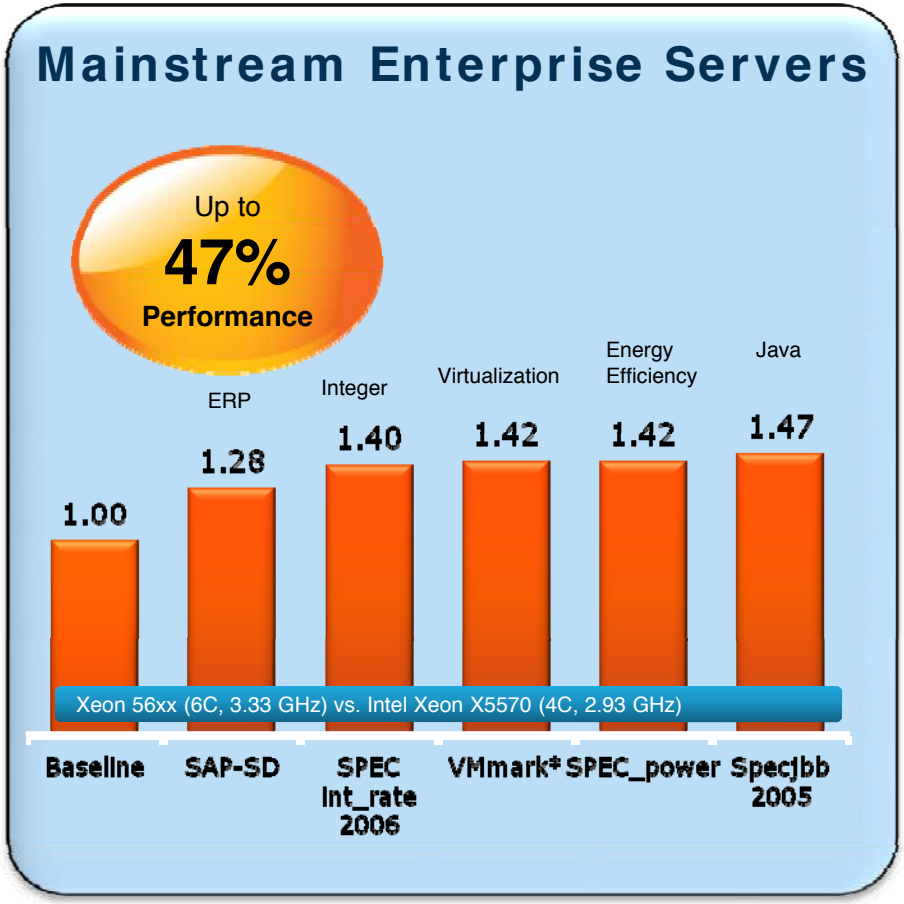
Westmere Xeon-56xx

Xeon® 56xx (Westmere) SKUs

Xeon® 5500 (Nehalem) SKUs

Intel® Xeon® Processor 56xx Series
Measured Silicon System Performance Summary





Up to 63% performance boost over Xeon® 5500

Sources : Core count, Cache size, 2-bins of Frequency

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/limits.htm

Source: Intel Internal measurements March 30, 2010.

Security

AES-NI – why not a CISC operation?

- AES defines 3 different key sizes:
  - 128/192/256 bit
  - Which take 10/12/14 algorithm calculation rounds respectively
- AES has a large number of modes (ECB, CBC, CTR, GCM, XTS, XTW, etc.)
- Could have built a single CISC instruction to do AES encrypt/decrypt :
  - Severely complicated flow. Potential export implications.
  - Might have picked the wrong modes, key sizes, etc.
- Split the AES operations into components
  - Forward cipher: AESENC, AESENCLST
  - Equivalent Inverse Cipher: AESDEC, AESDECLST
  - Key generation, matrix manipulation: AESIMC and AESKEYGENASST
  - Carryless multiply : CLMUL

AESNI Whitepaper at Intel.com (see last foil)

AES Encryption Flow

aeskeygenasst

- Key Generation / expansion

pxor

- First round is just an XOR

aesenc

- Next N rounds are aesenc (N varies for 128-, 192- and 256- bit key sizes)

aesenclst

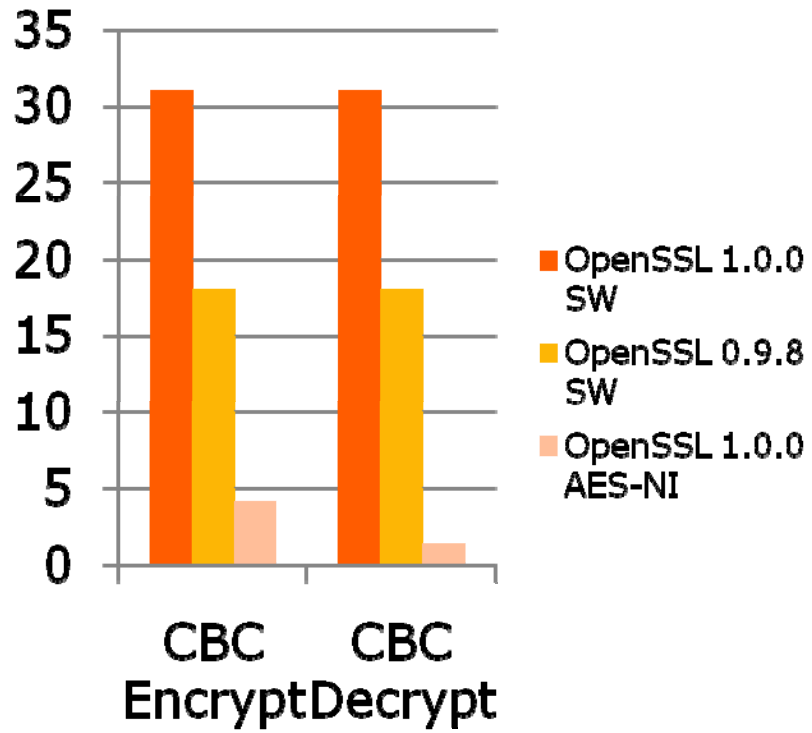
- Last round is aesenclst

AES-NI Perf

openssl –speed –evp **aes-128-cbc**

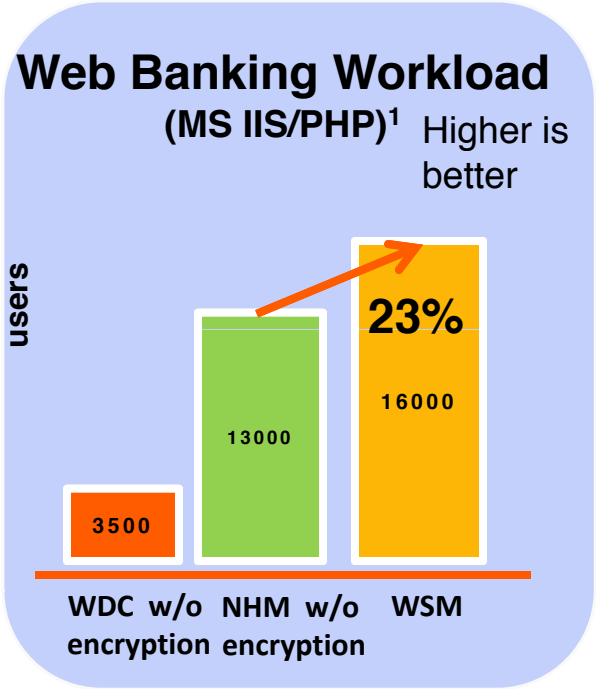
cycles/ byte measured on WSM 1C/ 1T

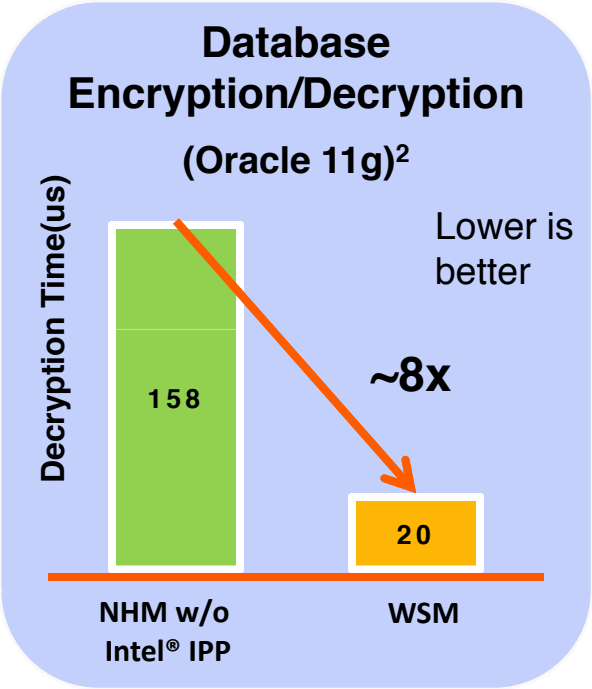
- Up to 8x cycles/byte raw improvement
  - OpenSSL Secure Socket Layer 1.0.0
- Execute with SSE operations:
  - AES at 16-bytes is natural fit for SSE HW.
  - Side-channel hardened (meaning operation timing / cache behavior is independent of secrets being protected).
- Enabled SW (BitLocker*, PGP*, TrueCrypt*, WinZip* ...) seeing significant benefits (next foil)

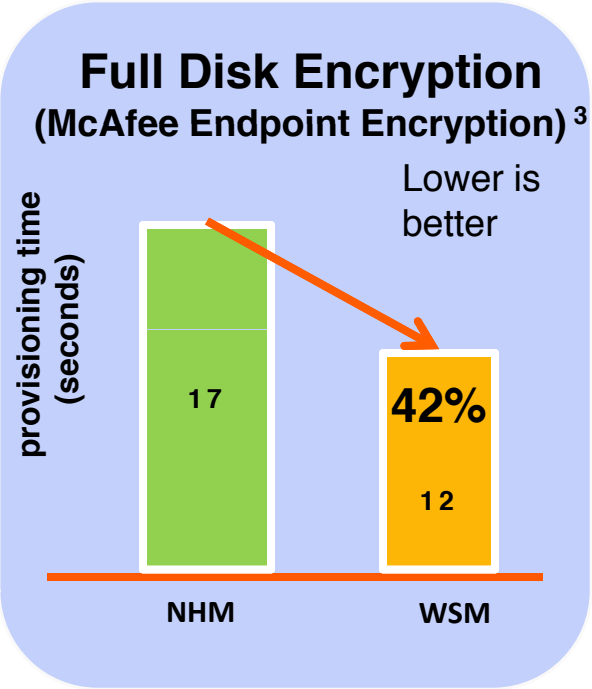


- OpenSSL 1.0.0 is "side-channel" hardened, so it is the appropriate comparison. SSL is Secure Socket Layer used for internet communication.
- 0.9.8 is shown for completeness
- CBC Encrypt is representative of a "serial" cipher mode. CBC Decrypt is representative of a "parallel" cipher mode. SW does not achieve pipelining in the decrypt case like the hardware.

Intel® Xeon® 56xx Series AES Encryption Performance







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 Intel Performance Benchmark Limitations.

1 Windows 2008 R2 x64 Enterprise Server. PHP banking sessions /users measured with Intel® Xeon® X5680 processor (WSM, 3.33 GHz) vs Inel® Xeon® 5160 processor (Woodcrest, 3 GHz) and Intel® Xeon® X5570 processor (NHM, 2.93 GHz), 24 SSD RAID 0 arrays, TLS_RSA_with_AES_128_CBC_SHA cipher suite.

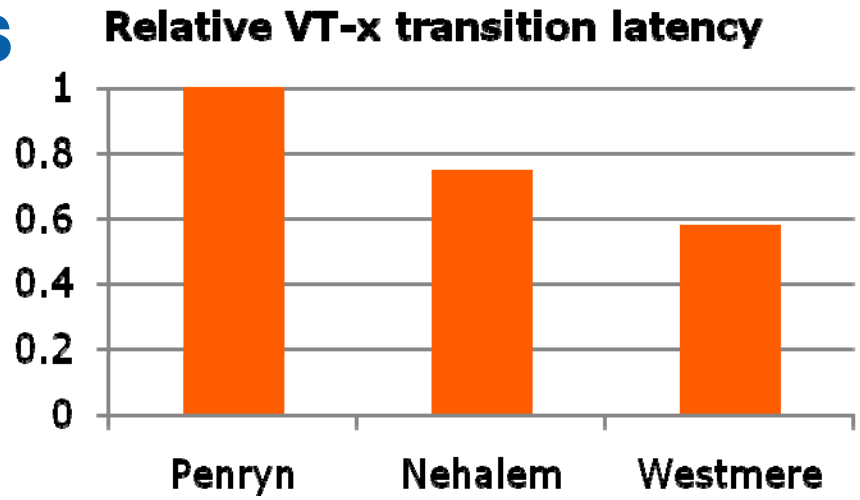
2 Oracle 11g with TDE, time takes to decrypt a 5.1 million row encrypted table with AES-256 CBC mode on Intel® Xeon® X5680 processor (WSM, 3.33 GHz) optimized with Intel® Performance Primitives crypto library (IPP) vs Intel® Xeon® X5560 processor (NHM, 2.8 GHz) without IPP. Timing measured is per 4K of data.

3 McAfee Endpoint Encryption for PCs (EEPC) 6.0 package with McAfee ePolicy Orchestrator (ePO) 4.5 encrypting a 32GB X25E SSD with Intel® Xeon® X5680 processor (WSM, 3.33 GHz) vs. Intel® Xeon® X5570 (NHM, 2.93 GHz). 24GB of memory.

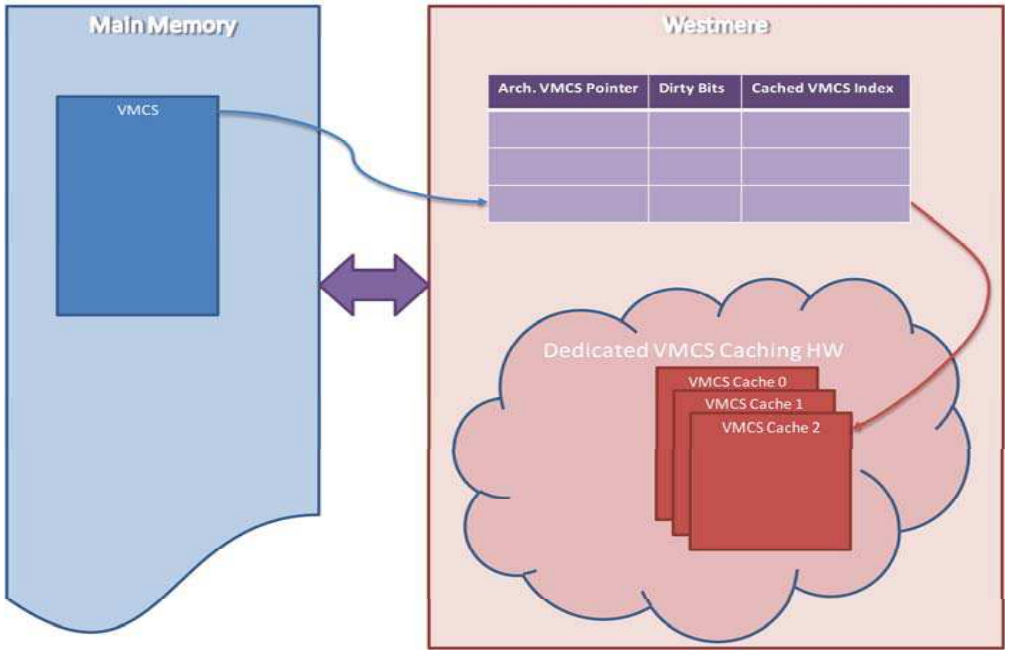
Virtualization

VT-x Improvements

- VT-x transition latency reduction:
  - Up to three VMCS's (virtual machine control structure) now cached in private SRAM on die.
  - Contains architectural state and VMX controls.
  - Previously cached only portions of the one currently active VMCS.

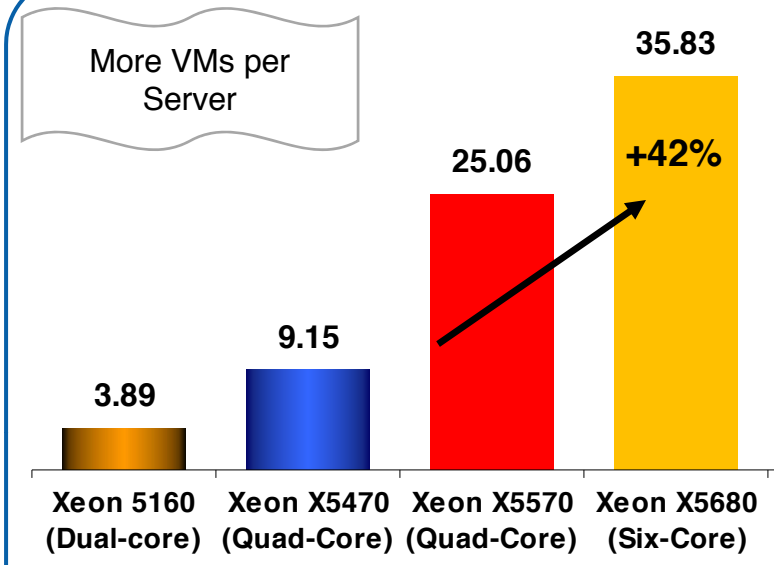


- VMX Architecture Enhancement "Unrestricted Guest" Mode
  - Allows VM guests to be in Real-Mode and unpaged protected mode.
  - Removes the need for a Real-Mode interpreter in VMM.
  - Significant boot time reductions for certain guests.



Intel® Xeon® Processor 56xx series based Server platforms

Virtualization performance on VMware ESX* using VMmark* benchmark



VMmark*

Higher is better

Leading X5680 Result by CISCO UCS B200 M2* Server

VMmark* is a VMware™ Virtualization benchmark Results are posted at

http://www.vmware.com/products/vmmark/results.html

Benchmark Description: VMmark* is designed as a tile-based benchmark consisting of a diverse set of workloads commonly found in the datacenter, The workloads comprising each tile are run simultaneously in separate virtual machines at load levels that are typical of virtualized environments. The performance of each workload is measured and then combined with the other workloads to form the score for the individual tile. Multiple tiles can be run simultaneously to increase the overall score.

A tile is a collection of six diverse workloads concurrently executing specific software. Running on one of two separate operating systems (Windows or Linux), each workload runs in its own virtual machine and executes specific applications. Included in a single tile are a web server, file server, mail server, database, Java server, as well as an idle machine. Results are posted at http://www.vmware.com/products/vmmark/results.html

Up to 42% gain on VMmark* over Xeon 5570

Source: Published/submitted/approved results as of March 30, 2010.

Westmere Xeon-56xx

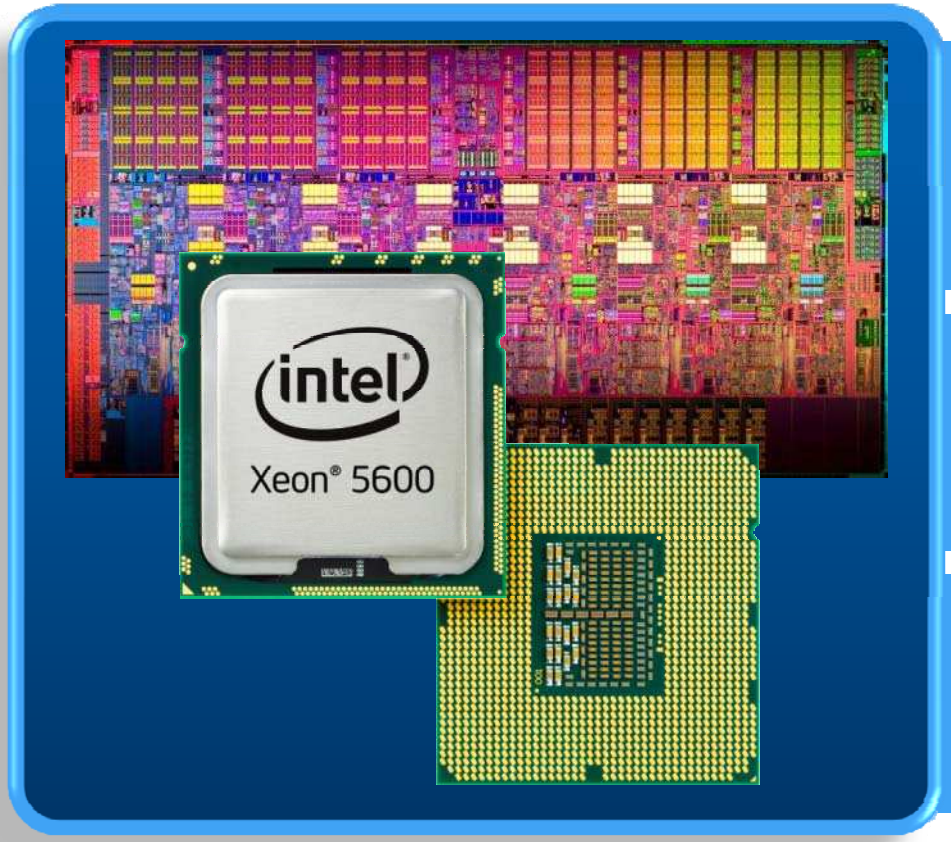
Power Efficiency Summary

Westmere Xeon-56xx

- 32nm Process and Scalable Architecture Enabled :
  - 50% more cores, 50% more L3 cache
  - Same or higher max frequencies as 45nm Nehalem cores
  - Similar to 4 core Nehalem power envelopes. 60w – 95w
  - Similar Idle power
  - OR
  - 4 cores in lower power envelopes. 45nm 80w ➔ 32nm 40w

- Key new features, and refinement of the NHM tock
  - Lower power DDR3L 1.35v dimm support
  - Higher peak memory bandwidth and 2DPC @ 1333
  - AESNI and TXT Measured Launch Security improvements.
  - VTx latency and real-mode support improvements.

Intel® Xeon® Processor 56xx Series



Better Energy Efficiency
with same performance as X5570 and up to 30% lower power[1]

Performance Leadership
with up to 60% performance boost over Xeon® 5500 servers[2]

More Secure
with Intel® AES New Instructions and Intel® Trusted Execution Technology

Intel® 32nm Process

1 Source: Fujitsu Performance measurements comparing Xeon L5650 vs X5570 SKUs using SPECint_rate_base2006.
See http://docs.ts.fujitsu.com/dl.aspx?id=a1400b1ff-56e2-4f26-a01c-2808e80cde52 and http://docs.ts.fujitsu.com/dl.aspx?id=4ef7ee10-2d91-4d9-bb3b-9cdf6177389
2 Source: Internal Intel measurements for Xeon® X5680 vs Xeon® X5570 on BlackScholes*.
3 Source: Intel measurements based on SPECjbb2005 performance comparison using server side java bops (business operations per second). Results have been estimated based on internal Intel analysis and are provided for informational purposes only.

For notes and disclaimers, see performance and legal information slides at end of this presentation.

Backup

Westmere Xeon-56xx – Overview

Actively shipping

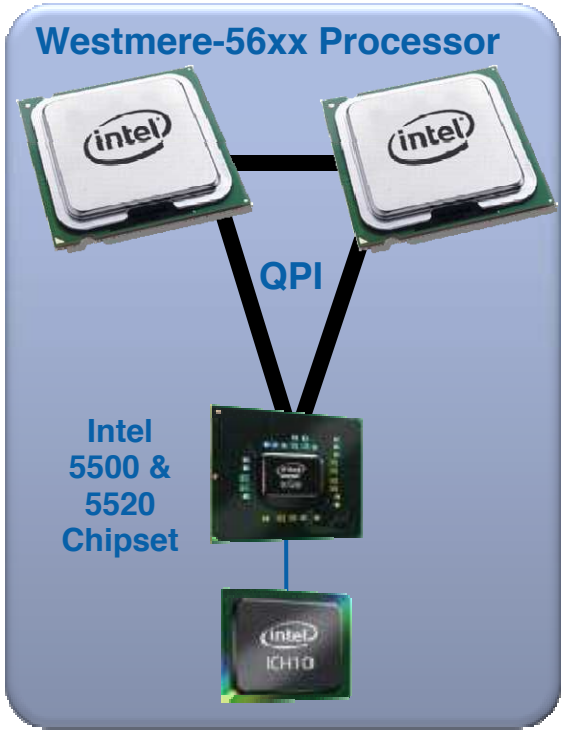
- Westmere-56xx

Up to 6 core/12 Thread

12 MB shared L3 cache

3 channels of DDR3, 3L memory support

AES, TXT, Improved Virtualization support



Socket: (same as NHM)
- LGA 1366 Pin Socket

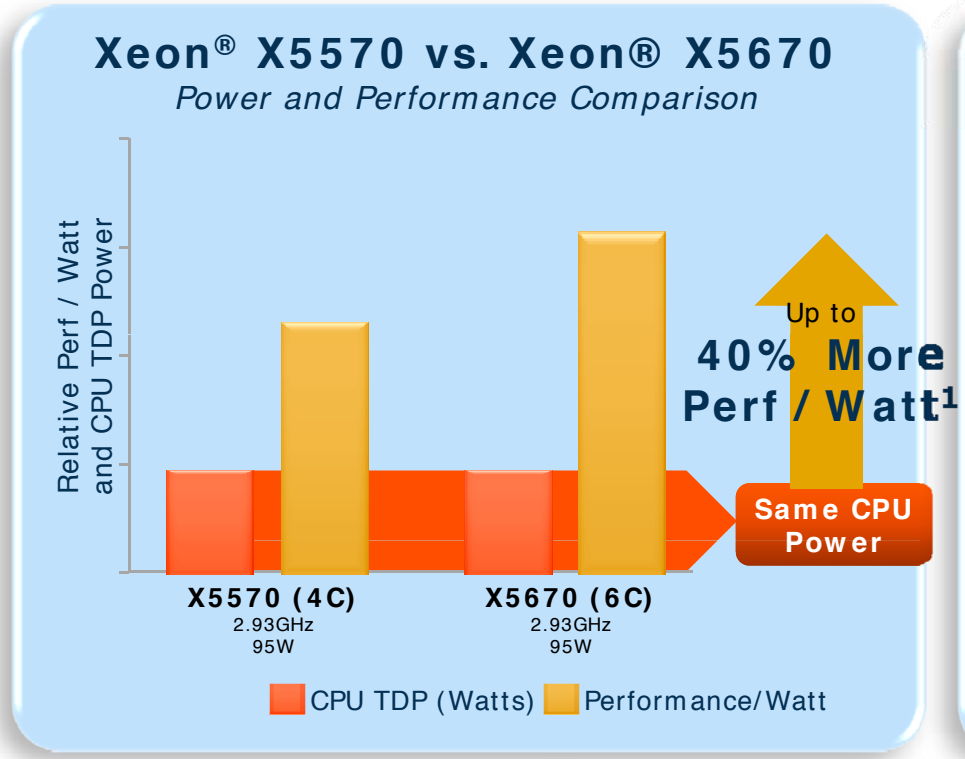
Process Technology:
- 32nm CPU

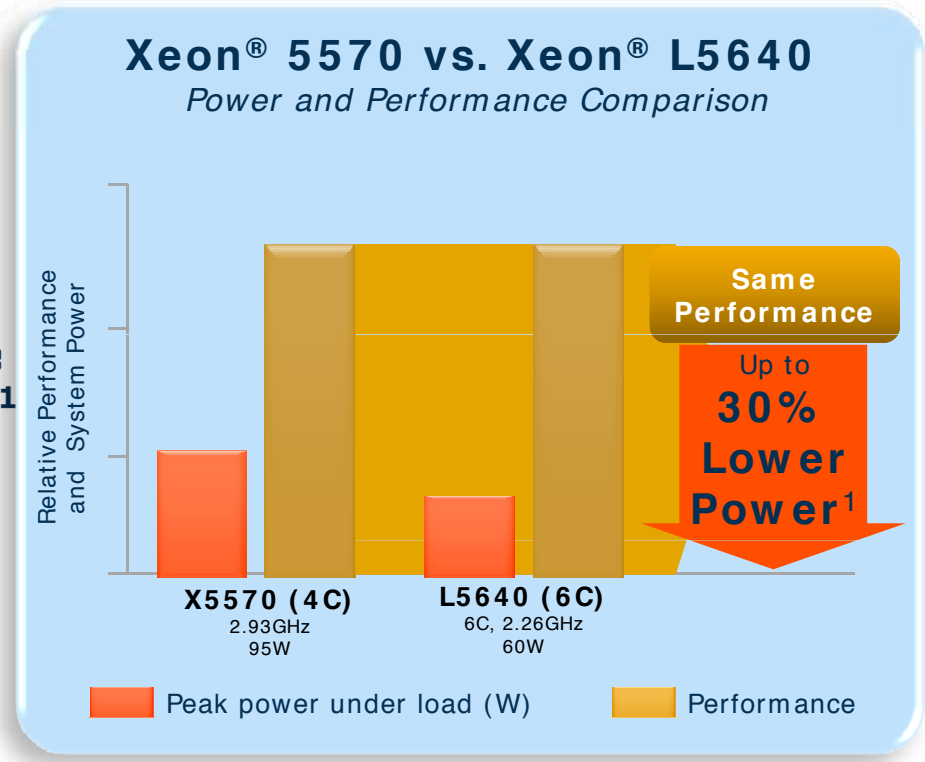
Platform Compatibility:
- Intel® 5500 & 5520 Chipset

Power:
- 130W down to 40W
- Adds 1.35v DDR3L support

Socket & Pin Compatible with Xeon 5500 Platforms with Additional Cores, Cache and 32nm Enhancements

Greater Datacenter Energy Efficiency





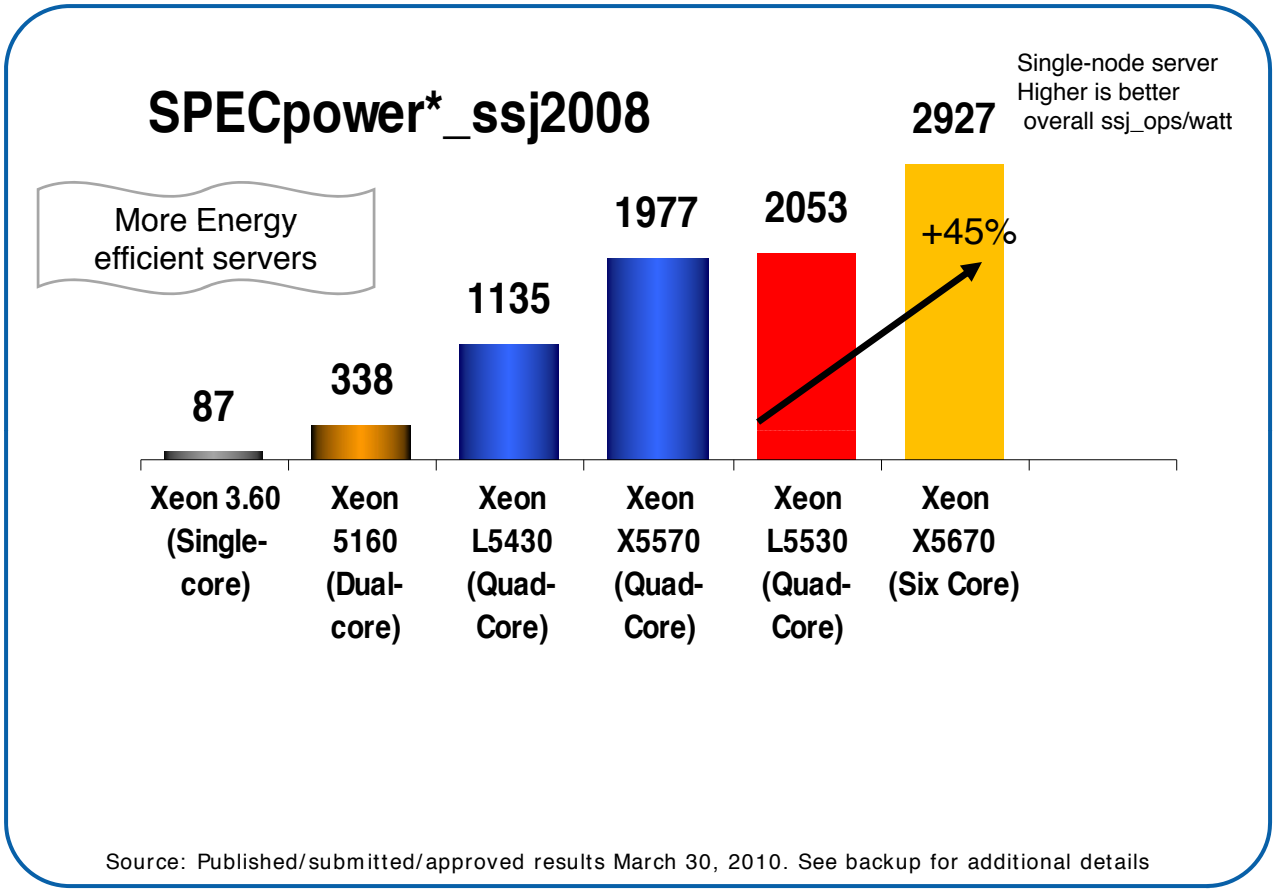
Maximize Performance or Energy Efficiency

[1] Source: Internal Intel estimates comparing Xeon® X5670 vs. X5570 SKUs using SPECpower. See backup for system configurations.

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/limits.htm

Intel® Xeon® Processor 5600 series based Server platforms

Energy Efficient performance on SPECpower*_ssj2008



Source: Published/submitted/approved results March 30, 2010. See backup for additional details

- Comparison basis: X86 architecture based DP Server platforms
- Leading result by IBM on IBM System x 3650 M3 server platform on Xeon X5670
  - IBM J9* JVM
  - Microsoft Windows Server 2008 Enterprise*

Benchmark notes:

- Measures energy efficiency of volume servers
- First industry standard bmk to measure power consumption in relation to performance across a "graduated" workload (11 different load levels -100%, 90%, 80% down to 0%)
- Measures platform power - AC watts at the wall
- Metric: Overall ssj_ops / watt (sum of the 11 perf points divided by sum of the 11 power points)

Xeon 5670 delivers all-time high SPECpower*_ssj2008 score

Xeon 3.60 – Intel® Xeon® Processor 3.60 1M L2 ("Nocona 3.60GHz", Single-Core)
Xeon 5160 – Intel® Xeon® Processor 5160 ("Woodcrest 3.0GHz", Dual-Core)
Xeon 5470 – Intel® Xeon® Processor L5430 ("Harpertown 2.66GHz", Quad-Core)
Xeon 5570 – Intel® Xeon® Processor X5570 ("Nehalem-EP 2.93GHz", Quad-Core)
Opteron 3435 – Six Core "Istanbul"
Opteron 6174 – Magny Cour

ISV Energy Efficiency Proof Points

ISV	Market Segment & Application	Xeon 5600 vs. 5500 series
Giant*	Giant is the one of the biggest online game vendor in China. Juren online game is the newest game developed by Giant	+30%
IBM*	IBM DB2 is a database Application. Hybrid data server for both XML and relational data	+29%
Kingsoft*	Kingsoft JXIII Online Game Server is next generation online game	+52%
Neusoft*	Neusoft CT &Pacs is key digital health solution focusing on X-ray computed tomography medical image processing	+37%
SAP*	The SAP ERP application (ECC 5.0) is an integrated software that addresses business requirements of mid and large orgs	+36%

Intel® Xeon® processor 5600 series delivers energy efficiency leadership with performance per Watt up to +52%

Intel® Xeon® 5600 Performance Records*

*As of May 28, 2010

Benchmark	Percentage gain over Xeon 5500	Result published by
Vmmark*	42%	Cisco
•• Multi-node SPECpower* _ssj2008	42%	HP
•• TPC Benchmark* E	35%	HP
•• SPECjEnterprise* 2010	33%	IBM
•• Single-node SPECpower* _ssj2008	33%	IBM
•• SPECjAppServer* 2004	30%	Cisco
•• SAP-SD* 2-Tier	28%	HP
•• SPECWeb* 2005	25%	Fujitsu
•• TPC Benchmark* C	21%	HP
•• SPEComp* Mbase2001	20%	Cisco
•• SPECint* _base2006	10%	Fujitsu

Over NINE New x86 2S Server & Workstation World Records

Westmere Xeon 56xx

Seven AES Instructions

Round Instructions:

AESENC xmm, xmm/m128: Encrypt one round

AESENCLAST xmm, xmm/m128: Encrypt last round

AESDEC xmm, xmm/m128: Decrypt one round using equivalent inverse cipher

AESDECLAST xmm, xmm/m128: Decrypt last round using equivalent inverse cipher

Key Manipulation Instructions:

AESIMC xmm, xmm/m128: Inverse mix columns

AESKEYGENASST xmm, xmm/m128, imm8: Generate next key from source material as indicated by imm8

Carryless Multiply:

CLMUL XMM, XMM, imm8 Carry less multiplication of 64 bits (as selected by the imm8) out of the two XMM registers returning a full 128 bit result.

Documentation at intel.com

Sample Code – Encrypt Round (ECB)

```
  mov ECX, $1                    ;; initialize key/round counter
  mov XMM1, PLAINTEXT            ;; load the plaintext to encrypt
  pxor XMM1, KEYSCHEDULE[$0]

aesloop:
  AESENC XMM1, KEYSCHEDULE[ECX]
  inc ECX
  cmp ECX, $0x9                  ;; 10 rounds in AES128
  ja aesloop
  AESENCLAST XMM1, KEYSCHEDULE[ECX]
  mov CIPHERTEXT, XMM1
```

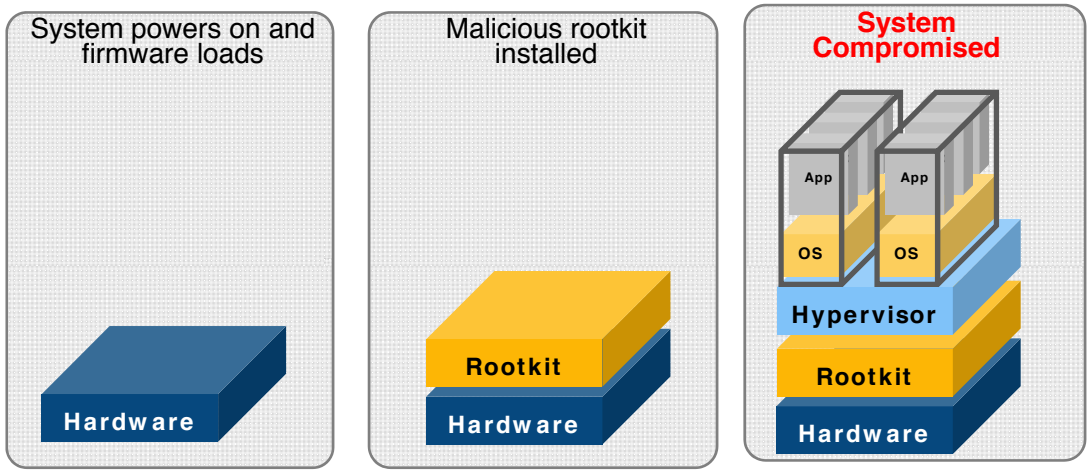
Sample Code – Round Key Generation (128-bit)

```
AESKEYGEN XMM1, INPUTKEY, 0x0        ;; gen ROUND 0 key
movdqa KEYSCHEDULE[0x0], XMM1        ;; store key
AESKEYGEN XMM1, XMM1, 0x1    ;; gen the ROUND 1 key
movdqa KEYSCHEDULE[0x1], XMM1        ;; store key
AESKEYGEN XMM1, XMM1, 0x2    ;; gen the ROUND 2 key
...
```

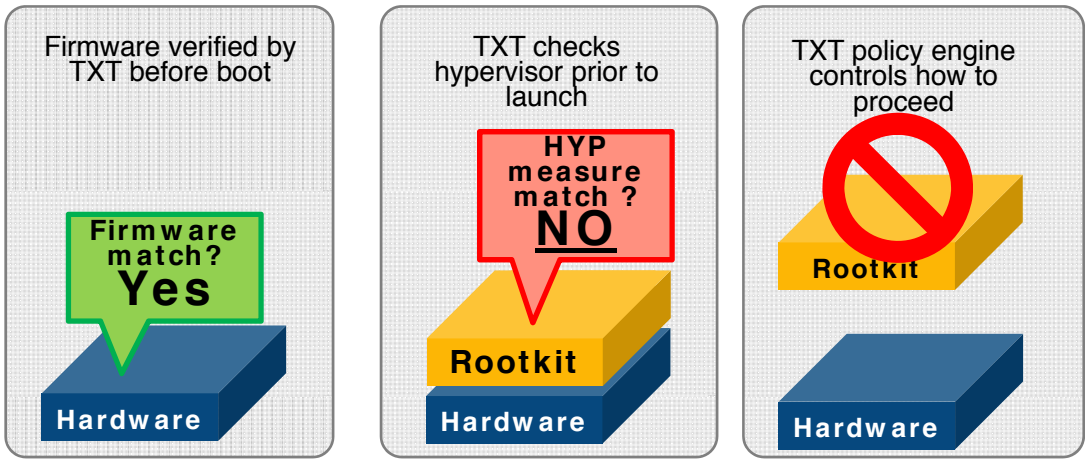
192 & 256 bit key generation are also supported

Intel® Trusted Execution Technology

Rootkit Attack Without TXT



Rootkit Attack With TXT



TXT helps prevent :

- **Firmware attacks**
- **Rootkit attacks**
- **Side-Channel attacks**
- **SMM attacks**
- **Power-on attacks**

Westmere Adds FIT boot to TXT

FIT Boot
Threat:
Unauthorized modification of the BIOS Boot
Functions:
Measures all regions of the BIOS specified
If assets in memory (i.e., secrets set) Verify that BIOS is authorized
If not: Brick
Adds signature-based BIOS verification
Scales TXT to large platforms
Security Benefit:
SINIT can gain assurance security-related patches were done.
Reduces a threat (i.e., un-authorization of the BIOS) into a denial of service.

SCLEAN
Threat:
Unauthorized modification of BIOS Boot Block exposes assets after a crash
Functions:
Scrubs memory after crash
Security Benefit:
Boot environment has assurance that rogue BIOS cannot access assets

SENTER/SINIT
Threat:
Subversion of kernel image on "disk"
Functions:
Deterministic Launch
Verified Platform Configuration
Security Benefit:
Untrusted components cannot interfere with MLE's measurement or launch control

STM (SMM Transfer Module)
Threat:
Rogue SMI handler provides attack pad
Functions:
Shim SMI handler with policy engine
Security Benefit:
Kernel can evaluate threat of SMM to the assets
Evaluation of trusted SMM component (STM) is feasible where evaluation of BIOS SMI is not feasible.

Yellow features existed prior to Westmere as part of TXT.

TXT – What is it

- **T**rusted e**X**ecution **T**echnology :
  - Works by creating a Measured Launch Environment (MLE)
  - MLE enables accurate HW based checks of TXT-enabled BIOS, hypervisor, or O/S environments via an cryptographically unique identifier for each approved launch-enabled software component.
  - Allows CPU HW check of boot environment or hypervisor launch code signatures against known good ones stored in a secure Trusted Platform Module (TPM) to prevent rogue firmware and BIOS attacks from gaining control of the system.
  - Stops launch of Firmware and Software which does not have the correct prescribed checksum expected.
  - Launch Control Policy tools decide on next system actions
- Westmere adds TXT system runtime firmware measurement
  - Allows BIOS and RAS feature setup to be included in the MLE

Detailed TXT whitepaper on Intel.com (see last foil)

Acronyms Glossary

Westmere-EP = **E**fficient **P**erformance = Xeon-5600 series
VR = Voltage Regulator
RC = Resistive Capacitance
TTM = Time to Market
DB = Database
LGA = Land Grid Array (packaging technology)
TXT = Trusted Execution Technology
L3$ = Level 3 cache (also called LLC for Nehalem, Westmere = Last Level Cache)
XSnp = cross-snoop. A coherency function and filter whereby the uncore knows and checks the subset of on-die core caches that may have copies of a system address.
UnCore = areas of chip which are not the converged client-server CPU core.
CR3 = IA register which allows a context switch when written
IDI = In-Die-Interface. The core-uncore communication interface. Allows low-latency dynamically variable voltage and frequency domain jumps.
VM = Virtual Machine. A software based version of a machine.
VMM = Virtual Machine Monitor. The supervisor of a virtual machine.
WDC = WoodCrest platform. A FSB based Core2™ Merom / Penryn era platform.
PCU = Power Control Unit
AES = Advanced Encryption Standard
VTx =
Additional References :
AESNI at http://www.intel.com/technology/security/downloads/323587.pdf
AESNI at http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/
Intel Trusted Execution Technology : visit http://www.intel.com/technology/security