AMD Opteron™ and Intel® Xeon® x86 processors in industry-standard servers

Technology brief, 2nd edition

Introduction

HP ProLiant and BladeSystem servers use multi-core AMD Opteron™ and Intel® Xeon® x86 processors. This technology brief describes some of the key processor technologies that we use as building blocks to construct balanced server architectures. Balanced server architectures deliver the highest price-to-performance and value for the virtualization, HPC, and database markets.

We use the designations "1P" for single-processor, "2P" for dual-processor, and "MP" for multi-processor servers with two or four processor sockets. For more information about HP ProLiant servers, visit www.hp.com/servers/technology.

Microarchitecture

Microarchitecture refers to the internal processor design, such as the number of cores that implements an instruction set. AMD and Intel constantly increase the number of cores, but they differ in their approach to using them. AMD provides more processor cores to run multi-threaded applications, with each core executing a single thread. Intel increases processor utilization by using Hyper-Threading Technology to execute two threads per core.

Intel Core Microarchitecture Nehalem and Westmere

Intel builds its Nehalem and Westmere microarchitectures on hafnium-based Hi-k metal gate silicon technology. This material reduces electrical leakage and allows for smaller, more energy-efficient, and higher performance processors. Nehalem (45 nm) and Westmere (32 nm) Xeon processors described in this paper support some or all of the following technologies:

- Three-level cache hierarchy supplies an on-die 64-KB L1 cache, an individual 256-KB L2 cache for each core, and a shared, inclusive 4 to 12 MB L3 cache.
- An integrated memory controller supports two or three DDR3 SDRAM memory channels or four FB-DIMM2 channels.
- Intel Hyper-Threading (HT) Technology improves processor utilization by letting each core execute two threads simultaneously.
- QuickPath links connect the processors and I/O chipset (see "I/O architecture").
- Integrated PCI Express and DMI replaces the northbridge in mid-range models.
- Trusted Execution Technology (TXT) increases protection against software-based attacks (see "Data security").
- Advanced Encryption Standard-New Instructions (AES-NI) allows fast and secure data encryption of a variety of applications. (See "Data security").
- Turbo Boost Technology increases the clock frequency of all active cores when the processor operates below pre-set power and thermal design limits. It complements HT Technology.
- Intel Virtualization Technology (VT) helps hardware to reduce software virtualization overhead (see "Virtualization").
- Dynamic Power Management works with Turbo Boost to increase performance and optimize the power use of the processor, chipset, and memory.
- Intel Machine Check Architecture Recovery, an advanced reliability feature, lets the OS continue to run even after it detects uncorrectable errors.

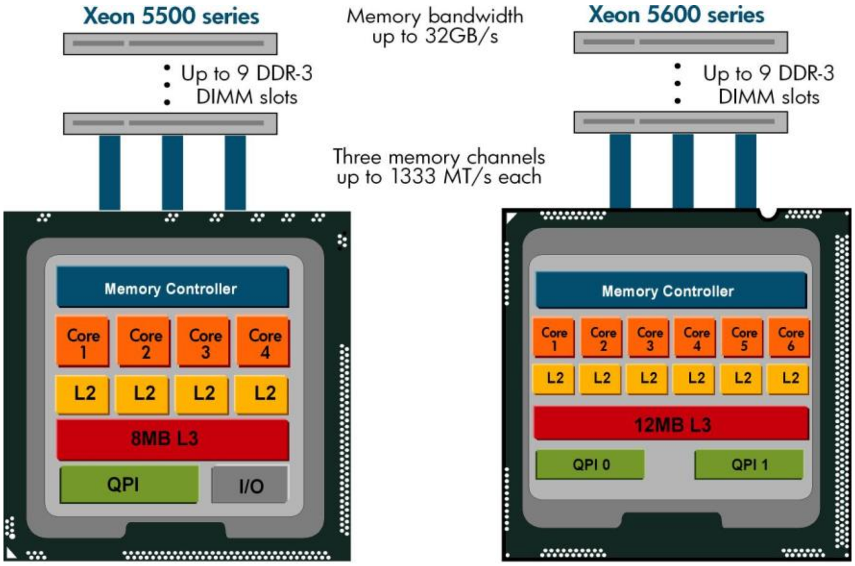
Processors for 1P and 2P ProLiant servers

We use Xeon 5500 and 5600 series processors in HP ProLiant 100, 200, 300, and 400 series servers. The Xeon 5500 series processor has six cores that share an 8-MB L3 cache (Figure 1). Intel uses the 45-nanometer (nm) manufacturing process to produce the processor.

By contrast, the Xeon 5600 series processor has eight-cores that share a 12 MB L3 cache. The L3 cache duplicates data in each core's L1 and L2 caches and stores it outside the cores. The L3 cache also eliminates unnecessary core snoops to the L1 and L2 caches. Intel uses the 32-nm process to produce the Xeon 5600 series.

Both 5500 and 5600 series processors contain an integrated memory controller. The controller uses three channels to access up to nine DDR3 memory sockets. The memory channels can operate up to 1333 MT/s (32 GB/s total), depending on the number and type of DIMMs in the slots.

Figure 1: Block diagrams of Xeon 5500 series processors and 5600 series processors



See a listing of 60-W, 80-W, and 95-W Xeon 5500 series processors and specifications at http://ark.intel.com/MySearch.aspx?s=t&CodeNameText=Nehalem-EP&MaxTDPMin=60&MaxTDPMax=95.

See a listing of 60-W, 80-W, 95-W, and 130-W Xeon 5600 series processors and specifications at http://ark.intel.com/MySearch.aspx?s=t&CodeNameText=Westmere-EP&MaxTDPMin=80&MaxTDPMax=130.

We use Xeon 6500 series processors in select 2P ProLiant G7 servers. These processors have four, six, or eight cores. Each processor contains a four-channel integrated memory controller. It has 64 KB L1 and 256 KB L2 caches for each core and a shared L3 cache of up to 18 MB. The processors use scalable memory buffers that support up to 16 memory slots per socket, or up to 1 TB using 16 GB DDR3 DIMMs in four-socket systems. The processors also include Intel Machine Check Architecture Recovery.

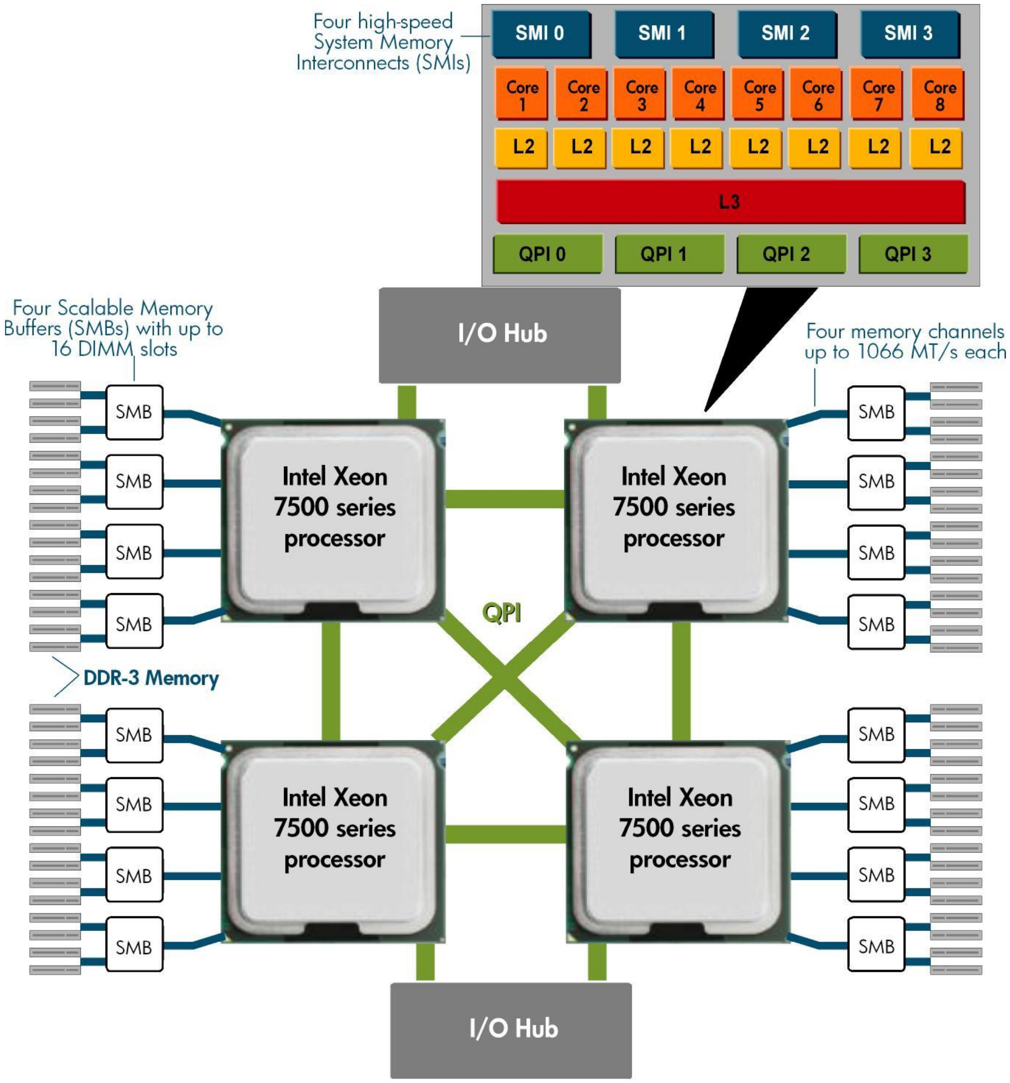
Xeon 6500 series processors include 105-W and 130-W versions. See the processor specifications at http://www.intel.com/p/en_US/products/server/processor/xeon6000/specifications.

Some 2P ProLiant G7 servers support E7-2800 series processors. The Xeon E7-2800 series processor has from six to ten cores and a shared, inclusive L3 cache of up to 30 MB. It has a four-channel integrated memory controller that supports up to 32 DIMM slots through four scalable memory buffers. The processors use QPI links to connect to the I/O hubs and to each other.

Processors for MP ProLiant servers

We use Xeon 7500 series processors in select MP ProLiant DL 500-series, BL600 series servers and MP ProLiant DL900 series G7 servers. The Xeon 7500 series processor has four, six, or eight cores and a shared, inclusive L3 cache of 24 MB. A four-channel integrated memory controller supports up to 16 DIMM slots through four scalable memory buffers (Figure 2). Four-socket ProLiant DL 500-series servers with Xeon 7500 series processors have 64 DIMM slots and support up to 1 TB of memory. The processors use QPI links to connect to the I/O hubs and to each other. The links include reliability, availability, and serviceability (RAS) features. The Xeon 7500 series processors support Intel Machine Check Architecture Recovery.

Figure 2: Block diagram of MP server platform using eight-core Xeon 7500 series (Nehalem-EX) processor


Four high-speed System Memory Interconnects (SMIs)
SMI 0
SMI 1
SMI 2
SMI 3
Core 1
Core 2
Core 3
Core 4
Core 5
Core 6
Core 7
Core 8
L2
L3
QPI 0
QPI 1
QPI 2
QPI 3
Four Scalable Memory Buffers (SMBs) with up to 16 DIMM slots
I/O Hub
Four memory channels up to 1066 MT/s each
SMB
Intel Xeon 7500 series processor
QPI
DDR-3 Memory
I/O Hub

All Xeon 7500 series processors support Intel HT technology and Intel VT. All except the four-core E7520 processor support Intel Turbo Boost Technology. Xeon 7500 series processors do not support Intel AES-NI or Intel TXT security technologies.

See a listing of 95-W, 105-W, and 130-W Xeon 7500 series processors and specifications at http://ark.intel.com/MySearch.aspx?s=t&CodeNameText=Nehalem-EX&MaxTDPMin=80&MaxTDPMax=130.

Some ProLiant DL900, DL 500, BL600c series G7 servers support the Xeon E7-4800 series processor. The E7-4800 series processor has from six to ten cores and a shared, inclusive L3 cache of up to 30 MB. A four-channel integrated memory controller supports up to 32 DIMM slots through four scalable memory buffers (Figure 3). The processors use QPI links to connect to the I/O hubs and to each other.

Intel Core Microarchitecture Sandy Bridge

The Sandy Bridge microarchitecture uses the 32-nm manufacturing process. The microarchitecture includes processors with four, six, or eight cores. It also features an integrated northbridge, memory controller, and graphics processing unit (GPU). Except where noted, the processors support the following technologies:

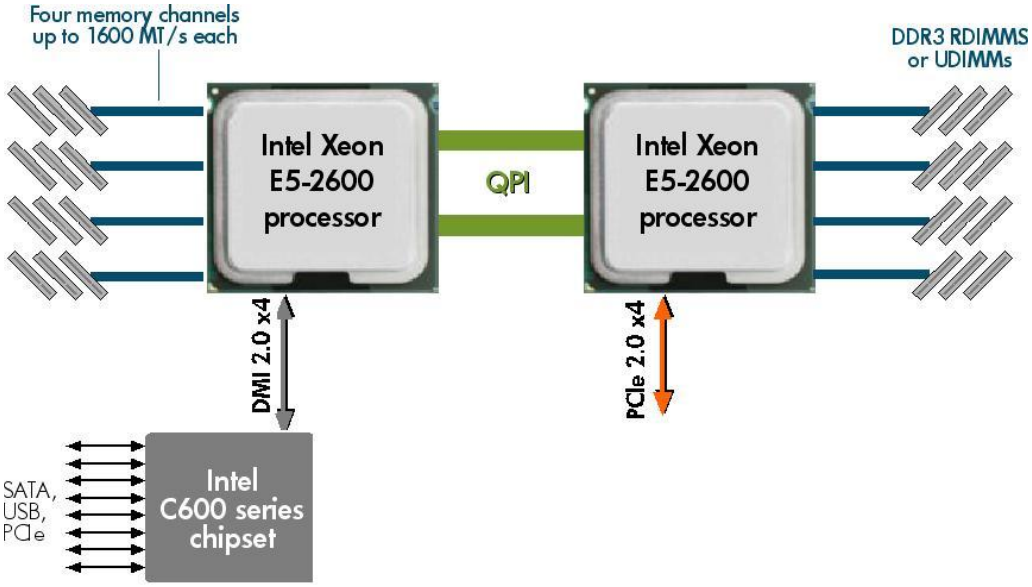
- Intel Hyper-Threading (HT) Technology
- Intel Virtualization Technology
- Advanced Encryption Standard-New Instructions
- Intel Advanced Vector Extensions (AVX)
- Trusted Execution Technology
- Integrated HD graphics (not supported by all processors)

Processors for 2P ProLiant servers

2P ProLiant Gen8 servers use Intel Xeon E5-2600 series processors (Figure 3) that operate from 60 W (Xeon LP) to 135 W. The processors include a 32K L1 instruction cache, 256 KB L2 cache per core, 20 MB L3 cache, two QPI links, and four Direct Media Interface (DMI) 2.0 lanes. The integrated four-channel memory controller supports up to three DDR3 DIMMs per channel with data rates up to 1600 MT/s. The processors work with RDIMMS, UDIMMS, LV-DIMMS, and load-reduced (LR) DIMMs.

The x4 DMI link is a bi-directional chip-to-chip interconnect between the processor and chipset, providing a total of 20 Gb/s in each direction, or 2.5 GB/s per unidirectional lane.

Figure 3: Block diagram of the 2p server platform using Xeon E5-2600 series processors


Four memory channels up to 1600 MT/s each
DDR3 RDIMMS or UDIMMs
Intel Xeon E5-2600 processor
QPI
Intel Xeon E5-2600 processor
DMI 2.0 x4
PCIe 2.0 x4
SATA, USB, PCIe
Intel C600 series chipset

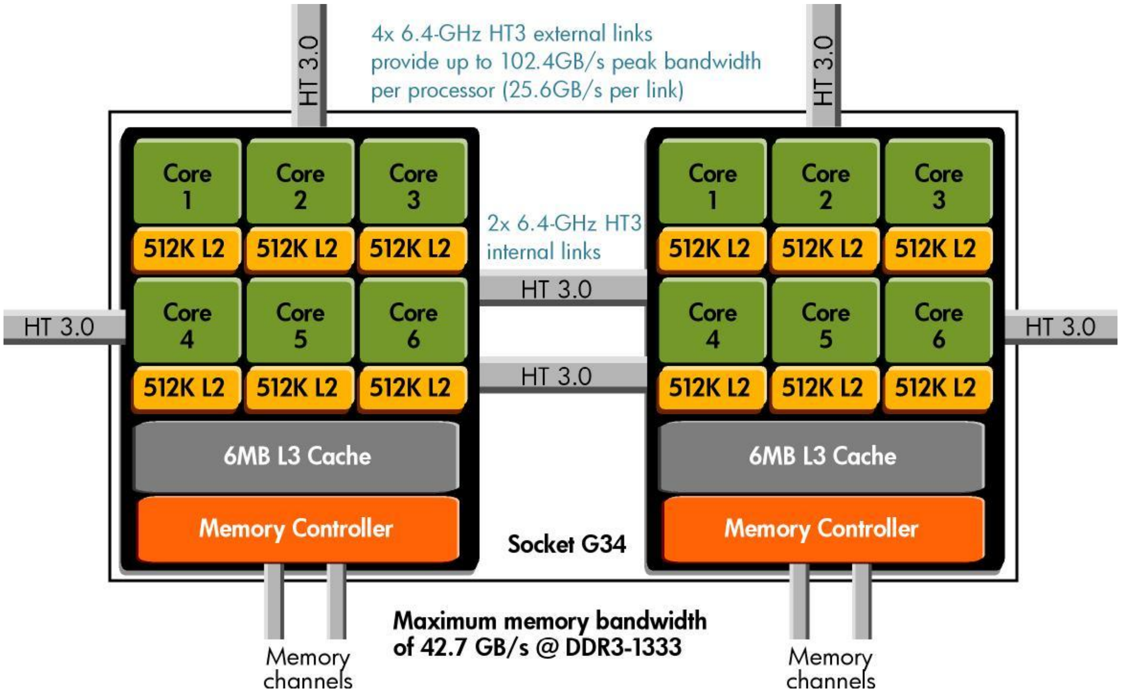
AMD Magny-Cours microarchitecture

We use AMD Opteron 6100 series processors with 8 or 12 cores in select 2P and 4P ProLiant servers. AMD produces the 8- and 12-core 6100 series processors with a 45-nm process. The processors feature Direct Connect Architecture 2.0 and contain two dies on a single multi-chip module (MCM) package (see Figure 4).

Each die has four or six cores, four Hyper Transport 3.0 links, and an integrated, dual-channel memory controller that supports up to three DDR3 DIMMs per channel at 1333 MT/s. Each core has an L1 Cache (64 KB for data and 64 KB for instructions), a 512 KB L2 cache, and a shared 6 MB L3 cache.

The 8-core and 12-core AMD Opteron processors run at speeds of up to 2.4 GHz and 2.3 GHz, respectively. They operate from 80 W to 105 W according to AMD. The processors fit into the 1944-pin G34 socket and use the AMD SR5690/SP5100 chipset.

Figure 4: Block diagram of the AMD Opteron 6100 series processor containing two 45-nm dies, each with four or six cores, 512-KB L2 cache per core, a shared 6-MB L3 cache, and four HT3 links



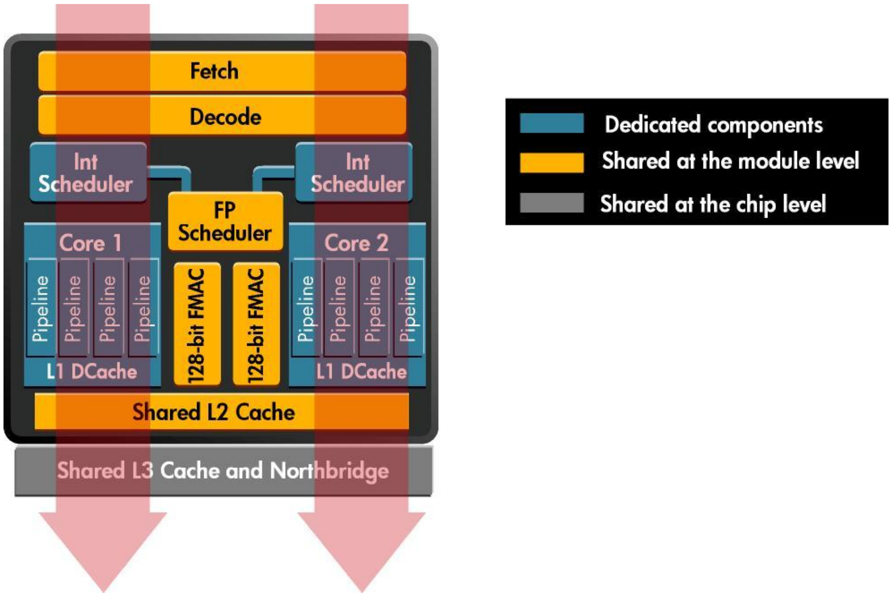
The AMD Opteron 6100 series processors support the following technologies:

- HyperTransport (HT) Assist, also called a probe filter, increases performance of AMD Opteron processor-based systems with four or eight sockets. It maintains data correctness, or coherence, between the processors and minimizes inter-processor communication traffic on the HyperTransport links.
- AMD Smart Fetch Technology lets cores enter a "halt" state during idle processing times, allowing them to draw less power. Data moves from the L1 and L2 caches to the shared L3 cache before going into the halt state. This allows the system to retrieve the contents of the idle cores.
- AMD-P suite of power-management features helps reduce energy use and cost (see "Power management").
- AMD-V™ with Rapid Virtualization Indexing reduces software virtualization overhead. (See "Virtualization").

AMD Bulldozer microarchitecture

We use AMD Opteron processors with 8 or 16 cores in select 2P and 4P ProLiant G7 servers. The building block of 8-core Opteron 4200 series and 16-core Opteron 6200 series processors is the Bulldozer module (Figure 5). The Bulldozer module executes two parallel threads using two 128-bit integer cores. Each core has four pipelines and a dedicated integer, but they share the fetch/decode stage and the L2 cache. The flexible floating point unit can be dedicated or shared between the two cores per cycle.

Figure 5: Block diagram of the AMD Bulldozer module with each core executing a single thread

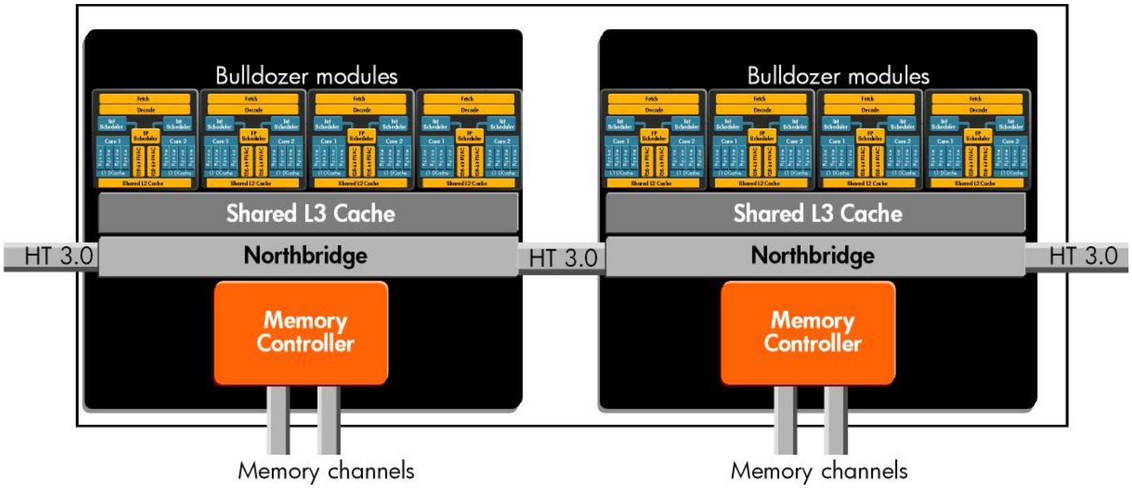


The Opteron 6200 series processor has 8 Bulldozer modules, runs from 1.6 GHz up to 2.6 GHz, and operates from 85 W up to 140 W. The Opteron 4200 series processor has 4 Bulldozer modules, runs from 2.1 up to 3.0 GHz, and operates from 85 W up to 115 W according to AMD. Both processors fit into the 1944-pin G34 socket and use the AMD SR5690/SP5100 chipset.

The AMD Opteron 6200 series processor (Figure 6) consists of two 8-core dies with four Hyper Transport 3.0 links that operate up to 6.4 GT/s. It has two integrated memory controllers, each with two DDR3 memory channels that operate up to 1866 GT/s. The memory controllers support LR DIMMs, RDIMMs, UDIMMs, and low-voltage DIMMs.

We use 8-core AMD Opteron 4200 series processors in select 2P ProLiant servers. The processor has a single dual-channel memory controller that operates up to 1600 GT/s.

Figure 6: Block diagram of the 16-core AMD Opteron processor with two dies, each with four Bulldozer modules



The AMD Opteron 4200 and 6200 series processors support the following technologies:

- HT Assist
- AMD Smart Fetch Technology
- AMD-P suite of power-management features (see “Power management”)
- AMD-V™ with Rapid Virtualization Indexing (See “Virtualization”)

Instruction set architecture

AMD Opteron and Intel Xeon processors adhere to the x86 instruction set architecture and are compatible with most 32-bit software applications. The x86-instruction set includes all instructions in the original 16-bit 8086 processor and enhanced instructions in succeeding x86 processors.

32-bit operations

A 32-bit processor has general-purpose registers (GPRs) 32 bits wide. The 32-bit processor can operate on an integer data stream that is 32 bits wide. The processor can also hold 32 bits of memory address data in a single register, for a maximum of 4 GB of addressable memory.

The x86 architecture supports physical addressing extensions (PAE) that expand the address space to allow addressing to 36 bits. This gives a maximum of 64 GB of physical addressable memory. AMD Opteron and Xeon processors support 32-bit addressing and the 36-bit PAE.

As shown in Table 3, the 32-bit instruction set for both the Intel Xeon and AMD Opteron family processors includes:

- Standard x86 instructions that are general-purpose arithmetic functions
- Single Input Multiple Data (SIMD) Instructions that let one command work simultaneously on multiple data items. This includes Streaming SIMD Extensions (SSE), SSE2, SSE3, and SSE4a instructions.
- x87 floating point instructions

Table 3. 32-bit x86 instructions common to AMD Opteron and Intel Xeon processors

Instruction name	Description	Register type	Size of registers	Number of registers
Standard x86	Instructions for logical operations, arithmetic operations, and address calculations. Also has 16-bit index registers for memory pointers.	GPR	32-bit	8
MMX	Multimedia instructions that allow the processor to do 64-bit SIMD operations	MMX	64-bit	8
x87	Instructions for floating-point calculations	FP	80-bit	8
SSE, SSE2, SSE3, SSE4, SSE4.1, 4.2. and SSE4a	SSE improves upon the MMX instructions and allows processors to do 128-bit SIMD floating-point operations. SSE2 adds 64-bit parallel floating-point numeric support. It also adds new instructions to support 128-bit SIMD integer operations. SSE3 instructions include 13 instructions that accelerate performance of SSE technology, SSE2 technology and x87-floating-point math capabilities. SSE4 includes instructions for AMD K10 and Intel Core microarchitecture. SSE4.1 is a subset of 47 instructions available in Intel Penryn. SSE4.2, a second subset of seven instructions, is available in Nehalem-based Core i7. SSE4a instructions include two new SSE instructions introduced in AMD K10. SSE4a instructions also add support for unaligned SSE load-operation, which formerly required 16-byte alignment.	MMX	128-bit	8
AVX	Intel Advanced Vector Extensions (AVX) is a 256-bit instruction set extension to SSE and is designed for applications that are floating-point intensive.			

64-bit extensions

AMD's and Intel's 64-bit extensions—named AMD64 and Intel 64—allow 32-bit processors to run 64-bit operating systems and applications. The key advantage of 64-bit processing is that a system can address a flat memory space of up to 16 exabytes. While 32-bit architecture theoretically can allow access up to 64 GB of memory, most 32-bit applications use only a maximum of 4 GB. That is due to the cumbersome and slow nature of the process needed to access the remainder of the memory. The 64-bit extensions give you the benefit of 64-bit addressing at a lower cost than the new hardware and software required for a 64-bit processor.

The 64-bit extensions also provide a larger register set with eight additional general-purpose registers (GPR) and 64-bit versions of the existing registers. With 16 GPRs, 64-bit extensions supply additional resources that compilers can use to increase performance.

I/O architecture

The I/O architectures of AMD Opteron-based and Intel Xeon-based systems include high-speed, point-to-point interconnects. The devices—AMD HyperTransport 3.0 (HT3) and Intel QuickPath

Interconnect—move data to processors, memory, and I/O devices. They improve performance, simplify design, and facilitate scalable multiprocessing systems.

AMD HyperTransport 3.0 technology

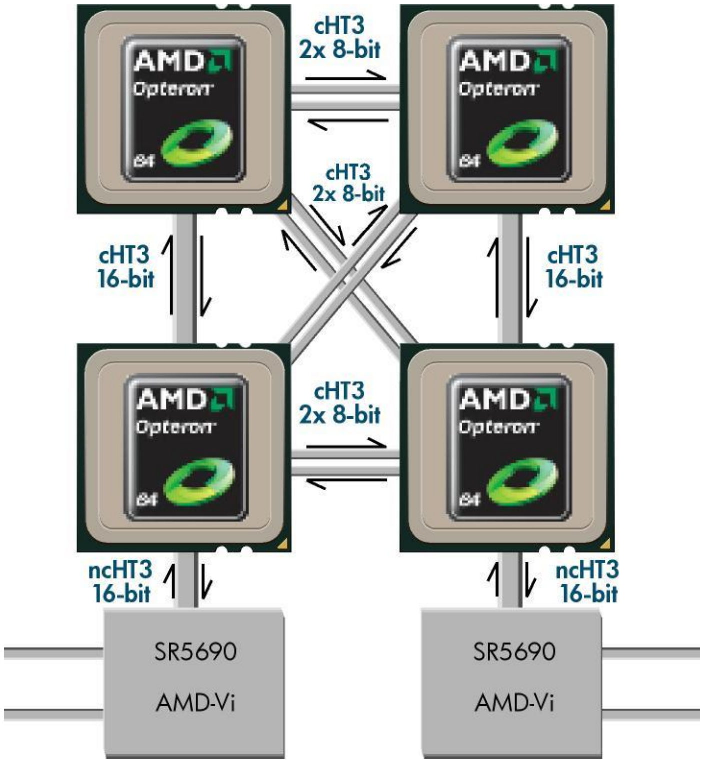
The HT3 interconnect consists of one 16-bit (wide) or two 8-bit (narrow) links. Each link has a maximum transfer rate of 6.4 gigatransfers per second (GT/s). This gives each wide link a maximum data rate of 6.4 GT/s × 2 bytes per transfer, or 12.8 GB/s. Each narrow link has a maximum data rate of 6.4 GB/s.

The HT3 links improve performance in 4P systems because the processors can communicate directly rather than moving data from one processor to another.

The AMD64 architecture uses a Non-Uniform Memory Access (NUMA) design to improve performance with multi-threaded applications. The NUMA design gives each AMD Opteron processor a local memory pool and then connects it to similar processors with their own memory pools. This design lets each processor access non-local memory. But access time varies based on memory pool location.

HT3 links can be coherent (cHT) or non-coherent (ncHT). Coherent links transfer cache coherency data. They connect two or more AMD Opteron processors and their memory pools. Non-coherent links move data between memory and I/O devices (see Figure 7).

Figure 7: Coherent HT3 links connect processors, and non-coherent HT3 links move data from memory to I/O devices.



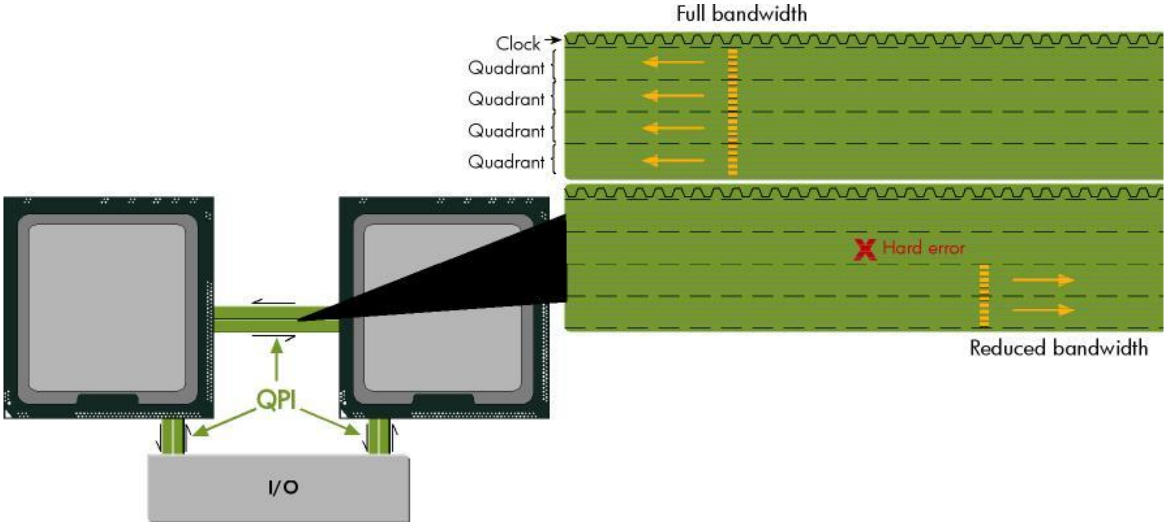
Intel QuickPath Technology

The QuickPath Interconnect (QPI) transmits data packets in parallel across two 20-bit links. Each link uses up to 16 bits (2 bytes) to transfer data and 4 bits for protocol and error correction. The QPI performs a maximum of 6.4 GT/s with 2 bytes per transfer, or 12.8 GB/s in each direction for a total theoretical bandwidth of 25.6 GB/s.

The QPI's reliability, availability, and serviceability (RAS) features include self-healing links and clock failover. Each 20-bit link divides into quadrants with five lanes each. As shown in Figure 8, if a persistent (hard) error occurs in one quadrant, the link automatically reduces its width to half (two quadrants) or quarter-width (one quadrant) using only the good lanes. This self-healing capability allows the interconnect to recover from multiple hard errors without data loss. Unrecoverable soft errors initiate a process to reduce the dynamic link width.

If the clock fails, the link reduces to half- or quarter-width, and the clock maps to a pre-determined data lane. The bandwidth of the link in RAS mode decreases, but the link in the other direction operates as usual.

Figure 8: Normal operation of QPI uni-directional link (top). A hard error reduces link bandwidth (bottom).



Power management

AMD and Intel multi-core processors contain power management features that maximize performance-per-watt and improve energy efficiency.

Intel Xeon power management

QuickPath Interconnect power

Xeon processors let QPI buffers enter a sleep state to reduce power requirements of inactive QPI links. ProLiant G6, G7, and Gen8 servers enable this feature by default. You can change it through the HP ROM-Based Setup Utility (RBSU). The Xeon processor determines when to put the QPI links into a low power state with minimal performance impact.

Disabling processor cores

Use the Core Disabling Options of the HP RBSU to disable either one core or half the cores in each Xeon 5500, 5600, or E5-2600 series processor. The disable command applies to all physical processors in the server. Engaging this capability saves power. It also may improve performance in servers running single workloads or with applications with low threading requirements.

Minimum processor idle power state

The Xeon 5500, 5600, and E5-2600 series processors support C-states for each core in the processor. C-states define the power state of system processors. They are an open specification of the ACPI group. The microarchitectures of the Xeon 5500, 5600, and E5-2600 series processors support processor C-states C0, C1, C3, and C6. C0 represents a fully active core executing instructions. The other C-states reduce power for idle cores. Any core in a processor can change C-states independently from the other cores.

You can set the maximum C-state for an idle processor through the RBSU. The OS initiates the C-state changes. The higher the C-state allowed at idle, the more power savings—but only at idle. Also, the higher the allowed C-state, the higher the latency involved when the core returns to activity.

AMD Opteron power management

AMD Opteron processors feature the AMD-P suite of power management technologies.

APML Remote Power Management Interface

The AMD Opteron 6-core 6100-series processor uses multiple thermal sensors to detect the processor's hottest part. Using a systems management device such as HP Integrated Lights-Out (iLO), you can remotely monitor and control P-state limits using AMD's APML Remote Power Management Interface. The iLO processor includes the processor thermal information in the data it sends to the fan controller.

Cool Speed™

Cool Speed technology protects processor integrity by reducing power states when the temperature exceeds an established safe limit and allows a server to continue operating. Cool Speed is enabled by default, and it is not a user option.

C1E™

In G34-based-systems, the northbridge chipset detects when all processor cores are idle and communicates it to the Southbridge chipset. The Northbridge and HT links power down, and the cores go into a deep sleep state. Depending on system configuration, this feature can yield a significant power savings. The OS manages C1E. You can enable or disable it through the HP RBSU.

Core Select Technology

This technology lets you select the number of active cores per processor through the HP RBSU (minimum of one, up to the full number supported). It can improve the performance of an application that was not designed to use the full number of cores. Reducing the active core count can increase memory bandwidth per thread.

PowerNow! Technology

AMD PowerNow! Technology with Independent Dynamic Core technology and Dual Dynamic Power Management™ allows a processor to run at different frequencies and voltages depending upon computing demand. As a result, PowerNow! can lower server power consumption without compromising performance. Activate it through the BIOS-controlled Dynamic Mode of Power Regulator for ProLiant.

Power Cap Manager

Power Cap Manager allows you to set a fixed limit on a server's processor power consumption by controlling the P-state of individual cores. The caveat is that a single voltage is supplied to all cores in the processor even if you request different P-states. In this instance, the actual P-state will equal that of the highest voltage required of the selected P-states. You can control this through HP Dynamic Power

Capping. You can access Dynamic Power Capping from iLO Advanced menus or the HP Insight Control (ICE) management suite.

AMD Turbo CORE technology

Thermal design power (TDP) represents the maximum power use of the processor. Processors rarely consume more than 70% of TDP for average workloads, so AMD uses Average CPU Power (ACP) to reflect what processors normally use. AMD Turbo CORE technology lets you take advantage of the headroom between TDP and ACP by allowing the processor to increase its clock speed until it reaches the TDP level. Turbo CORE is based on power use, not processor temperature. If the processor approaches TDP, Turbo CORE automatically reduces the processor's speed to ensure that it continues to operate within the specified guidelines. This capability enables significantly higher maximum clock speeds.

TDP Power Cap

TDP Power Cap lets you reduce the TDP of Bulldozer-based processors and adjust their frequency to meet power and workload demands. You can reduce the TDP of the processor to lower its power use and then tweak the frequency of the cores to get the maximum performance for that TDP setting. This allows you to add more server blades to a rack without significantly reducing performance.

Virtualization

In a virtual machine (VM) environment, a software layer known as the hypervisor makes it appear that each guest OS has full control over the server's processor, memory, and I/O devices. Actually, each guest OS has its own virtual processors, virtual drives, virtual NICs, and virtual storage controllers.

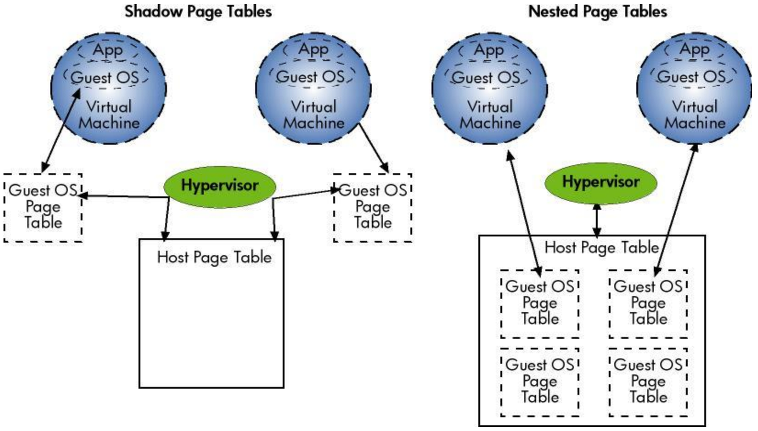
Several categories of software-layer abstraction exist. AMD-V and Intel VT technologies fall in the hardware-assisted-virtualization category. These technologies assist the hypervisor by removing the overhead associated with software-only virtualization.

AMD Virtualization Technology (AMD-V) 2.0

The VM's view of physical memory is different from that of the memory controller. The hypervisor dynamically translates the VM's memory addresses sent to and received from the memory controller. As a result, each VM application remains unaware that memory is being virtualized. This translation process, known as shadow paging, increases memory latency and degrades performance.

Rapid Virtualization Indexing, an AMD-V innovation, reduces software virtualization overhead. It introduces hardware support for a second (nested) level of address translation. Rapid Virtualization Indexing, also known as nested paging, uses nested page tables that the hypervisor sets up to improve guest OS performance, when compared to shadow page tables (Figure 9).

Figure 9: Hardware-based management using nested page tables improves the speed of the guest OS.



Virtualization enhancements with the AMD-V 2.0 include:

- Tagged Translation Look-aside Buffer (TLB)—Hardware features that facilitate efficient switching between virtual machines for better application responsiveness
- AMD-V™ Extended Migration—Hardware feature that helps virtualization software enable live migration of virtual machines between all processor generations

Intel Virtualization Technology (Intel VT)

Intel VT, a group of extensions to the x86 instruction set, consists of three technology suites. They work together to improve virtualization performance in a server's processor, chipset, and I/O devices.

Intel VT in Intel Xeon processors (Intel VT-x)

With software-only virtualization, the hypervisor must trap and execute certain instructions for the virtual, guest OS. Intel VT-x reduces these hypervisor interventions. It also helps transfer platform control between the hypervisor and guest OSs so that the handoffs are faster, more reliable, and more secure.

Intel VT for Directed I/O (Intel VT-d)

Intel VT-d reduces the need for the hypervisor to manage I/O traffic. Intel VT-d assigns specific I/O devices to specific guest operating systems. Intel VT-d gives each I/O device a dedicated area in system memory that only the device and its guest OS can access. This speeds data movement and decreases performance overhead.

Intel VT for Connectivity (Intel VT-c)

Intel VT-c integrates hardware assists into I/O devices like NICs and storage controllers. Intel VT-c is a collection of technologies that sorts an enormous variety of incoming data and sends it to its destination. By performing these functions in dedicated network silicon, Intel VT-c increases throughput and reduces the load on the hypervisor and server processors.

Data security

Virtualization has raised data security concerns because server workloads are no longer physically separated in the data center. These concerns have intensified with the growing threat of malicious software attacks aimed at the hypervisor, BIOS, and firmware. HP ProLiant G6 and G7 servers protect against these threats by adding the hardware-based security technology featured in the latest Intel Xeon and AMD Opteron processors.

Intel security technology

Intel Xeon 5600 and E5-2600 series processors use Advanced Encryption Standard New Instructions to provide hardware-based acceleration for secure transactions. The processors also use Trusted Execution Technology to enhance security through hardware-based resistance to malicious attacks.

Advanced Encryption Standard New Instructions (AES-NI)

AES-NI allows faster encryption and decryption performance. Read more about it at http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-aes-instructions-set/.

Trusted Execution Technology (Intel TXT)

Intel Trusted Execution Technology complements anti-virus software. It increases protection against software-based attacks to the hypervisor or BIOS and protects against malicious rootkit installations. Intel TXT creates a Measured Launch Environment (MLE) that lets you compare a system's critical launch components to approved code during the boot and launch sequence. Intel TXT detects any changes to the MLE and blocks any unapproved code from launching. Intel TXT establishes an optimal number of protected launch components called a root of trust, which is difficult to defeat or modify.

Intel TXT requires:

- Xeon 5600 or E5-2600 series processor and Intel TXT-enabled chipset
- Intel Virtualization Technology
- Authenticated Code Module
- Launch Control Policy tools
- Intel TXT-enabled BIOS
- Intel TXT-enabled hypervisor or OS
- Trusted Platform Module (TPM) v1.2

ProLiant servers with Xeon 5600 or E5-2600 series processors can use Intel TXT. We offer the technology as an option for select ProLiant servers that you may already own. We also offer the TPM microcontroller for select ProLiant servers that support Intel TXT. The TPM securely stores encryption keys, passwords, and digital certificates for platform authentication. It stores platform measurements that help keep the platform trustworthy.

AMD security technology

AMD Opteron processors contain a security instruction known as Security Kernel Initialization (SKINIT). It works with TPM to establish a secure environment for trusted software such as a hypervisor.

SKINIT helps to create a root of trust. It starts with an unsecure operating mode and reinitializes the processor to set up a secure environment for a software component called the secure loader. SKINIT executes the secure loader in an unalterable way. SKINIT also copies the secure loader image to the TPM for verification using unique bus transactions. The transactions prevent malicious software from imitating the SKINIT operation in ways that TPM could not detect.

Performance

It's difficult to compare the performance of AMD Opteron and Intel Xeon architectures because there are no absolutes about which processor will perform better in a given system. System performance includes more than just the processor. That's one reason we design ProLiant and BladeSystem servers with a balanced architecture that maximizes system performance. A balanced architecture requires superior engineering of the processor, memory, I/O, storage, and networking subsystems.

We regularly conduct the following benchmark tests to gauge the performance of our ProLiant and BladeSystem platforms:

- **SPECpower_ssj™ 2008** compares the energy efficiency of servers and determines the amount of power that servers require at different usage levels.
- **SPEC CPU2006** focuses mainly on compute-intensive environments in mathematics and the sciences and less on business workloads.
- **TPC-C** simulates an Online Transaction Processing (OLTP) database environment.
- **VMmark** measures the performance of virtualized servers.
- **SAP® Sales and Distribution (SD) standard application benchmark** tests the hardware and database performance of SAP applications and components.
- **TPC-H** simulates a Decision Support System or Business Intelligence database environment.

In general, our latest benchmark tests show the AMD Opteron-based 4P ProLiant DL585 G7 server as the top-ranked choice for virtualization/consolidation environments and corporate data center infrastructures. The Intel Xeon-based 4P ProLiant DL580 G7 server scored highest on the two-tier SAP SD standard application benchmark with SAP enhancement package 4 for the SAP ERP application 6.0. The Intel Xeon-based ProLiant DL380 G7 and AMD Opteron-based DL385 G7 come in first in performance and price-to-performance, respectively, on the 100GB TPC-H benchmark.

You can review recent benchmark tests of our server platforms at http://h18004.www1.hp.com/products/servers/benchmarks/new.html. Still, benchmarks only produce snapshots of the relative level of performance you can expect. For the most accurate results, you should test a server platform in your own business environment.

Conclusion

This paper summarizes the technologies in the latest generation of AMD Opteron and Intel Xeon processors. These technologies include:

- Microarchitecture
- I/O
- Power management
- Virtualization
- Data security

We use these technologies to construct balanced architectures in G6, G7, and Gen8 ProLiant servers that deliver a wealth of HP innovations to reduce operating costs and accelerate business solutions.

For more information

Visit the URLs listed below if you need additional information.

Resource description	Web address
ProLiant servers home page	www.hp.com/servers/proliant
Intel Xeon 5600 Series Processor	www.intel.com/itcenter/products/xeon/5600/index.htm
Intel Xeon 5500 Series Processor	www.intel.com/itcenter/products/xeon/5500/index.htm
Intel Xeon 7500 Series Processor	www.intel.com/itcenter/products/xeon/7500/index.htm
Intel Xeon Processor E7 Family	http://www.intel.com/products/server/processor/xeonE7/index.htm
AMD Opteron 6000 Series Platform web page	www.amd.com/us/products/server/processors/6000-series-platform/Pages/6000-series-platform.aspx

Send comments about this paper to TechCom@HP.com.

Follow us on Twitter: http://twitter.com/ISSGeekatHP

TC1108813, March 2012