Intel Xeon 4214 processor

Artikel	110557
Herstellernummer	BX806954214
EAN	0735858415613
Intel	

Intel® Turbo Boost Technology

Intel® Turbo Boost Technology dynamically increases the processor's frequency as needed by taking advantage of thermal and power headroom to give you a burst of speed when you need it, and increased energy efficiency when you don't.

Intel® vPro™ Platform Eligibility

Intel® vPro™ Technology is a set of security and manageability capabilities built into the processor aimed at addressing four critical areas of IT security: 1) Threat management, including protection from rootkits, viruses, and malware 2) Identity and web site access point protection 3) Confidential personal and business data protection 4) Remote and local monitoring, remediation, and repair of PCs and workstations.

Intel® Hyper-Threading Technology

Intel® Hyper-Threading Technology (Intel® HT Technology) delivers two processing threads per physical core. Highly threaded applications can get more work done in parallel, completing tasks sooner.

Intel® Virtualization Technology (VT-x)

Intel® Virtualization Technology (VT-x) allows one hardware platform to function as multiple "virtual" platforms. It offers improved manageability by limiting downtime and maintaining productivity by isolating computing activities into separate partitions.

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

Intel® Virtualization Technology for Directed I/O (VT-d) continues from the existing support for IA-32 (VT-x) and Itanium® processor (VT-i) virtualization adding new support for I/O-device virtualization. Intel VT-d can help end users improve security and reliability of the systems and also improve performance of I/O devices in virtualized environments.

Intel® VT-x with Extended Page Tables (EPT)

Intel® VT-x with Extended Page Tables (EPT), also known as Second Level Address Translation (SLAT), provides acceleration for memory intensive virtualized applications. Extended Page Tables in Intel® Virtualization Technology platforms reduces the memory and power overhead costs and increases battery life through hardware optimization of page table management.

Intel® TSX-NI

Intel® Transactional Synchronization Extensions New Instructions (Intel® TSX-NI) are a set of instructions focused on multi-threaded performance scaling. This technology helps make parallel operations more efficient via improved control of locks in software.

Intel® 64

Intel® 64 architecture delivers 64-bit computing on server, workstation, desktop and mobile platforms when combined with supporting software.¹ Intel 64 architecture improves performance by allowing systems to address more than 4 GB of both virtual and physical memory.

Instruction Set

An instruction set refers to the basic set of commands and instructions that a microprocessor understands and can carry out. The value shown represents which Intel's instruction set this processor is compatible with.

Instruction Set Extensions

Instruction Set Extensions are additional instructions which can increase performance when the same operations are performed on multiple data objects. These can include SSE (Streaming SIMD Extensions) and AVX (Advanced Vector Extensions).

of AVX-512 FMA Units

Intel® Advanced Vector Extensions 512 (AVX-512), new instruction set extensions, delivering ultra-wide (512-bit) vector operations capabilities, with up to 2 FMAs (Fused Multiply Add instructions), to accelerate performance for your most demanding computational tasks.

Enhanced Intel SpeedStep® Technology

Enhanced Intel SpeedStep® Technology is an advanced means of enabling high performance while meeting the power-conservation needs of mobile systems. Conventional Intel SpeedStep® Technology switches both voltage and frequency in tandem between high and low levels in response to processor load. Enhanced Intel SpeedStep® Technology builds upon that architecture using design strategies such as Separation between Voltage and Frequency Changes, and Clock Partitioning and Recovery.

Intel® Speed Shift Technology

Intel® Speed Shift Technology uses hardware-controlled P-states to deliver dramatically quicker responsiveness with single-threaded, transient (short duration) workloads, such as web browsing, by allowing the processor to more quickly select its best operating frequency and voltage for optimal performance and power efficiency.

Zusammenfassung

Intel® Turbo Boost Technology

Intel® Turbo Boost Technology dynamically increases the processor's frequency as needed by taking advantage of thermal and power headroom to give you a burst of speed when you need it, and increased energy efficiency when you don't.

Intel® vPro™ Platform Eligibility

Intel® vPro™ Technology is a set of security and manageability capabilities built into the processor aimed at addressing four critical areas of IT security: 1) Threat management, including protection from rootkits, viruses, and malware 2) Identity and web site access point protection 3) Confidential personal and business data protection 4) Remote and local monitoring, remediation, and repair of PCs and workstations.

Intel® Hyper-Threading Technology

Intel® Hyper-Threading Technology (Intel® HT Technology) delivers two processing threads per physical core. Highly threaded applications can get more work done in parallel, completing tasks sooner.

Intel® Virtualization Technology (VT-x)

Intel® Virtualization Technology (VT-x) allows one hardware platform to function as multiple "virtual" platforms. It offers improved manageability by limiting downtime and maintaining productivity by isolating computing activities into separate partitions.

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

Intel® Virtualization Technology for Directed I/O (VT-d) continues from the existing support for IA-32 (VT-x) and Itanium® processor (VT-i) virtualization adding new support for I/O-device virtualization. Intel VT-d can help end users improve security and reliability of the

systems and also improve performance of I/O devices in virtualized environments.

Intel® VT-x with Extended Page Tables (EPT)

Intel® VT-x with Extended Page Tables (EPT), also known as Second Level Address Translation (SLAT), provides acceleration for memory intensive virtualized applications. Extended Page Tables in Intel® Virtualization Technology platforms reduces the memory and power overhead costs and increases battery life through hardware optimization of page table management.

Intel® TSX-NI

Intel® Transactional Synchronization Extensions New Instructions (Intel® TSX-NI) are a set of instructions focused on multi-threaded performance scaling. This technology helps make parallel operations more efficient via improved control of locks in software.

Intel® 64

Intel® 64 architecture delivers 64-bit computing on server, workstation, desktop and mobile platforms when combined with supporting software.[1] Intel 64 architecture improves performance by allowing systems to address more than 4 GB of both virtual and physical memory.

Instruction Set

An instruction set refers to the basic set of commands and instructions that a microprocessor understands and can carry out. The value shown represents which Intel's instruction set this processor is compatible with.

Instruction Set Extensions

Instruction Set Extensions are additional instructions which can increase performance when the same operations are performed on multiple data objects. These can include SSE (Streaming SIMD Extensions) and AVX (Advanced Vector Extensions).

# of AVX-512 FMA Units

Intel® Advanced Vector Extensions 512 (AVX-512), new instruction set extensions, delivering ultra-wide (512-bit) vector operations capabilities, with up to 2 FMAs (Fused Multiply Add instructions), to accelerate performance for your most demanding computational tasks.

Enhanced Intel SpeedStep® Technology

Enhanced Intel SpeedStep® Technology is an advanced means of enabling high performance while meeting the power-conservation needs of mobile systems. Conventional Intel SpeedStep® Technology switches both voltage and frequency in tandem between high and low levels in response to processor load. Enhanced Intel SpeedStep® Technology builds upon that architecture using design strategies such as Separation between Voltage and Frequency Changes, and Clock Partitioning and Recovery.

Intel® Speed Shift Technology

Intel® Speed Shift Technology uses hardware-controlled P-states to deliver dramatically quicker responsiveness with single-threaded, transient (short duration) workloads, such as web browsing, by allowing the processor to more quickly select its best operating frequency and voltage for optimal performance and power efficiency.

Intel Xeon 4214, Intel Xeon Silver, LGA 3647 (Socket P), 14 nm, Intel, 2.2 GHz, 64-bit

Intel Xeon 4214. Processor family: Intel Xeon Silver, Processor socket: LGA 3647 (Socket P), Processor lithography: 14 nm. Memory channels: Hexa-channel, Maximum internal memory supported by processor: 1.02 TB, Memory types supported by processor: DDR4-SDRAM. Market segment: Server, Supported instruction sets: SSE4.2, AVX, AVX 2.0, AVX-512, Scalability: 2S. Package type: Retail box. Processor package size: 76mm x 56.5mm

Merkmale

Logistics data

Harmonized System (HS) code	85423119

Memory

Maximum internal memory supported by processor	1.02 TB
Memory types supported by processor	DDR4-SDRAM

Operational conditions

Tcase	77 °C

Other features

Maximum internal memory	1 TB

Packaging data

Package type	Retail box

Weight & dimensions

Processor package size	76mm x 56.5mm

Graphics

On-board graphics card	No
Discrete graphics card	No
On-board graphics card model	Not available
Discrete graphics card model	Not available

Memory clock speeds supported by processor	2400 MHz
Memory channels	Hexa-channel
ECC	Yes

Technical details

Launch date	Q2'19
Product type	Processor
Status	Launched
Supported memory types	DDR4-SDRAM
Memory speed (max)	2400 MHz
Number of UPI links	2
Servicing status	Baseline Servicing

Features

Execute Disable Bit	Yes
Market segment	Server
Maximum number of PCI Express lanes	48
PCI Express slots version	3.0
Supported instruction sets	SSE4.2, AVX, AVX 2.0, AVX-512
Scalability	2S
Embedded options available	Yes
PCI Express CEM revision	3.0
Export Control Classification Number (ECCN)	5A992C
Commodity Classification Automated Tracking System (CCATS)	G077159

Processor

Processor manufacturer	Intel
Processor generation	2nd Generation Intel® Xeon® Scalable
Processor model	4214
Processor base frequency	2.2 GHz
Processor family	Intel Xeon Silver
Processor cores	12
Processor socket	LGA 3647 (Socket P)
Component for	Server/workstation
Processor lithography	14 nm
Processor threads	24
Processor operating modes	64-bit
Processor boost frequency	3.2 GHz
Processor cache	16.5 MB
Thermal Design Power (TDP)	85 W
Box	Yes
Cooler included	Yes
Processor codename	Cascade Lake
Processor ARK ID	193385

Processor special features

Intel® Hyper Threading Technology (Intel® HT Technology)	Yes
Intel® Turbo Boost Technology	2.0
Intel® AES New Instructions	Yes

(Intel® AES-NI)	
Enhanced Intel SpeedStep Technology	Yes
Intel Trusted Execution Technology	Yes
Intel® Speed Shift Technology	Yes
Intel® Transactional Synchronization Extensions	Yes
Intel VT-x with Extended Page Tables (EPT)	Yes
Intel TSX-NI	Yes
Intel 64	Yes
Intel Virtualization Technology (VT-x)	Yes
Intel Virtualization Technology for Directed I/O (VT-d)	Yes
Intel Turbo Boost Max Technology 3.0	No
AVX-512 Fused Multiply-Add (FMA) units	1
Intel® Deep Learning Boost (Intel® DL Boost)	Yes
Intel® Speed Select technology - Performance Profile (Intel® SST-PP)	No
Intel® Resource Director Technology (Intel® RDT)	Yes
Intel® Volume Management Device (VMD)	Yes
Intel® Run Sure Technology	No
Mode-based Execute Control (MBE)	Yes
Intel® Optane™ DC Persistent Memory Supported	No
Intel® vPro™ Platform Eligibility	Yes
Intel Speed Select Technology (SST)	No
Intel® Speed Select Technology - Base Frequency (Intel® SST-BF)	No
Intel® Optane™ DC Persistent Memory technology	No