1-800-633-1440
training@mindshare.com
www.mindshare.com

Intel Processor (Skylake/Kaby Lake) and Platform Architecture Training

Let MindShare Bring "Intel Processor and Platform Architecture" Course to Life For You

Each generation of core architecture Intel64 and IA-32 Instruction Set Architecture (ISA) platforms brings new capabilities while maintaining backward compatibility with earlier x86 family members. Building on features introduced in the earlier processors, the 22nm Haswell and 14nm Broadwell CPUs include a new microarchitecture and significant enhancements in areas including instruction throughput, power conservation, integrated graphics, and system-on-a-chip (SOC) packaging options. Follow-on 14nm CPUs include Skylake and Kaby Lake processor that add new enhanced features and provide better performance. This 5-day combination course covers both of the key Intel processor and platform elements while describing interactions between processor, memory, chipset and devices. The focus is on architecture, interactions, and initialization of the processor (CPU) and Platform Controller Hub (PCH) components.

Many CPU, PCH, and attached device features are managed as PCI functions—each with some combination of IO, MMIO, and PCI Configuration Space registers which are initialized by BIOS or other software. Arbor software demonstrations integrated into this course enable students to examine the decoded contents of PCI, IO, and MMIO registers and CPU model-specific registers (MSRs).

This course is updated as best ask possible to reflect the architecture of Intel's latest processors (Skylake/Kaby Lake) and platforms and is based on publicly available documents.

You Will Learn:

- Intel processor and platform variants: Desktop, Mobile and Server platforms. NUMA and implications on OS
- Platform addressing
- CPU internal architecture including caches
- Implications of HyperThreading
- Overview of CPU and PCH interfaces
- Overview of Virtualization support
- Interrupt handling
- CPU and Platform Management
- Performance Monitoring

Course Length: 5 days (but customizable to 4 days)

Course Outline:

- Intel Core Architecture CPU Background
  - Intel 64 and IA-32 CPU lineage: 80386 to Skylake/Kaby Lake
  - Haswell/Broadwell/Skylake/Kaby Lake Processor and Platform Examples
    - Desktop
    - Mobile/Tablet
    - Server (Hawell/Broadwell Xeon E5 processors without and with Cluster-On-Die (COD))
    - Non-Unified Memory Architecture (NUMA) and implications
- CPU Internal Architecture
  - Processor role: Fetch/Decode/Execute
    - Motivation for CISC to uOp decoding
    - Superscalar, parallel execution
  - CPU Resources: Dedicated vs. Shared
  - Instruction Pipeline Architecture Details
- x86 Instruction Set Background
- Intro to the Instruction Set
  - General Purpose Instructions
  - Floating Point and SIMD Instructions
    - x87, MMX, SSE, SSE2, SSE3, SSE4, AVX, AVX-2, AVX-512
  - Program Flow-related Instructions
  - Hardware-Related Instructions

1-800-633-1440
training@mindshare.com
www.mindshare.com

- Intro to the Register Set and Address Spaces
  - General Purpose registers (GPRs)
  - x87 / MMX registers
  - XMM / YMM / ZMM registers
  - Segmentation registers
  - Control registers
  - Debug registers
  - Model-Specific registers (MSRs)
  - Memory, IO, and Configuration Spaces
- Operating Modes
  - Real Mode
  - Protected Mode
  - Virtual-8086 Mode
  - System Management Mode
  - Long (IA32e) Mode
    - 64-bit Mode; REX prefixes
    - Compatibility Mode
- Real Mode Operation
- Introduction to Multitasking
- Segmentation (Protected Mode)
- Paging
  - Purpose of Paging
  - Paging Basics
    - Physical vs. Virtual (Linear) Address Space
    - Swap space (secondary storage)
    - x86 paging structures
      - Page Directory Entries (PDEs)
      - Page Table Entries (PTEs)
  - TLBs (Translation Lookaside Buffers)
    - Managing TLBs (INVLPG, PCID, VPID topics etc)
    - Global pages
  - x86 Paging Modes (features)
    - Page Size Extensions (PSE)
    - Physical Address Extensions (PAE)
      - 3-level lookup: Page Directory Pointer Entries (PDPE)
    - IA32e (Long) Mode Paging
      - 4-level lookup: Page Map Level 4 Entries (PML4E)
    - Execute Disable functionality
- Memory Management
  - Caches
    - Five Memory Types
    - Cache Policy Setup: MTRRs
    - Cache Policy Setup: Paging Structures
    - L1, L2, L3 Cache Hardware Architecture
    - CPU Rules Of Conduct: UC/WC and WB/WT/WP Regions
  - Miscellaneous Cache Topics:
    - PAT Feature
    - Software Prefetch Instruction
    - Non-temporal Data
    - Direct Data IO (DDIO) and Direct Cache Access (DCA)
    - Cache QoS, Cache Allocation Technology (CMT) and Cache Monitoring Technology (CAT)
  - Intel TSX (Transactional Synchronization eXtensions)
- Intro to Virtualization Technology (Intel-VT)
  - What is virtualization
  - Hardware extensions: Intel-VTx
    - VMX Root Mode (Host Mode) vs VMX non-Root Mode (Guest Mode)
    - Virtual Machine Control Structure (VMCS)
    - Intel-VT instructions (VMLAUNCH, VMRESUME, etc.) and #VMEXIT
  - Memory Management with Virtualization
    - Shadow Page Tables
    - Extended (Nested) Page Tables
    - TLB Management with Virtualization

1-800-633-1440
training@mindshare.com
www.mindshare.com

- Data Protection Extensions
  - Intel SGX (Software Guard eXtensions)
  - Intel MPX (Memory Protection eXtensions)
- Platform Addressing
  - Traffic types
    - Programmed IO (PIO)
    - Direct memory access (DMA)
    - Peer-to-Peer
  - System IO addresses
    - Legacy IO and limitations of IO space accesses
    - Accessing IO space CPU *IN and OUT* Instructions
  - System Memory Addresses
    - System DRAM Main Memory
    - Memory Mapped IO (MMIO)
    - Addressing Memory Space using CPU *MOV* Instructions
  - PCI Configuration Space
    - PCI topology rules and Bus/Device/Function (BDF) numbers
    - CPU access of PCI space: two methods
    - Legacy method: IO space access
    - Newer method: MMIO space access
- Overview of CPU and PCH Interfaces
  (key features of interfaces covered based on class requirements and time limitations)
  - QuickPath Interface (QPI)
    - Coherent Bus (Multiple-Socket CPU Systems)
    - Signaling Environment
    - Traffic Types
    - Source and Home Snoop Protocol
  - System DRAM Memory
    - Overview of DRAM Architecture including DDR3/DDR4
    - Terminology: RAS, CAS, Precharge, Refresh, Error handling, Bank, Rank, DIMM etc.
    - DRAM read/write access protocol
  - PCI Express (PCIe)
    - Gen1/Gen2/Gen3 Protocols
  - Direct Media Interconnect (DMI)
    - Dual-simplex CPU-PCH Connection
    - Bandwidth Considerations
  - Universal Serial Bus (USB) 2.0
    - Integrated PCH EHCI USB 2.0 Host Controllers and Rate Matching Hubs (RMH)
    - Support For Low, Full, High Speed USB Downstream Devices/Hubs
  - Universal Serial Bus (USB) 3.0
    - Integrated PCH xHCI USB 3.0 Host Controller
    - SuperSpeed USB 3.0 Devices/Hubs
    - Backward Compatibility with USB 2.0 Devices/Hubs
  - Serial ATA (SATA)
    - Integrated PCH SATA Host Controllers
    - Supported SATA Operational Modes/Rates
    - Intel Rapid Storage Technology (RST)
- Platform Interrupt Handling
  - IO APIC and Local APICs
  - Message Signaled Interrupt (MSI/MSI-X) basics
  - CPU Interrupt Servicing
- Miscellaneous CPU and Platform Management topics
  - Power Management
    - C-States, P-States, Intel SpeedStep, Intel Speed Shift
    - MWait and Monitor Instructions
  - Thermal Management
  - System Management Mode (SMM)
  - Error Handling and Machine Check Architecture (MCA)
  - Performance Monitoring (PM)
    - CPU Core PM
    - CPU Uncore PM
    - Precision Event Based Sampling (PEBS)

1-800-633-1440
training@mindshare.com
www.mindshare.com

Recommended Prerequisites: A basic understanding of computer architecture

Course materials:

1) Course presentation PDF
2) MindShare's "x86 Instruction Set Architecture" eBook by Tom Shanley
3) MindShare Arbor Software 14-day trail version