

Intel Processor (Ice Lake & Cascade Lake) and Platform Architecture

Training

Let MindShare Bring Intel x86 Processor and Platform Architecture to life for you

Each CPU and chipset generation brings new capabilities while maintaining backward compatibility with earlier platforms. New 9th and 10th generation CPU architectures offer significant improvements in instruction throughput, power conservation, integrated graphics, security, system-on-a-chip (SOC) packaging options, etc. This 5-day course introduces the x86 Instruction Set Architecture (ISA) and describes the hardware features of the latest Intel Core and Xeon CPUs supporting it. In addition, the course presents an overview of memory, platform controller hub (PCH) logic, and IO interfaces that may be employed when implementing common system types.

A full understanding of an Intel x86 hardware platform includes knowledge of CPU/PCH capabilities, BIOS/OS setup of programmable platform features, as well as the dynamic status of the system with regards to thermal and error events, etc. MindShare Arbor demonstrations integrated into this course present a decoded view of register setup, system and device status, as well as a coherent summary of platform information reported when the CPUID instruction is executed. Students may use Arbor software for real-time scans of local systems, read/modify specific registers, and even save Arbor scan results for later sharing and off-line review.

This course is updated as frequently as possible in an attempt to provide a “snapshot” of current Intel Core and Xeon x86 platform components and system implementations. Content is based on publicly available documents

You Will Learn:

- Intel x86 CPU and Chipset Evolution
- Current Core and Xeon CPUs: Ice Lake, Cascade Lake, plus “Refresh” Variants
- X86 Instruction Set Architecture (ISA) and CPU Operating Modes
- Core and Xeon CPU Microarchitecture Differences
- Caches
- Platform Addressing
- Main Memory DRAM
- Ultra Path Interconnect (UPI)
- CPU Integrated Graphics
- CPU Integrated IO (IIO)
- Interrupt Handling
- Hardware Virtualization Support
- Platform Controller Hub (PCH) Features
- Power and Thermal Management
- CPU Performance Monitoring

Course Length: 5 Days, but customizable to 4 days (or other course durations)

Course Outline:

- Intel x86 Core and Xeon Platform Background
 - Intel 64 and IA-32 CPU lineage
 - 80386 to Ice Lake/Cascade Lake
 - Core and Xeon CPUs Expected Next
 - Ice Lake/Cascade Lake Platform Examples
 - Gaming Desktop
 - 2-in-1 Laptop
 - Xeon Scalable CPU Server

- X86 Instruction Set Architecture (ISA)
 - CPU Core Fetch/Decode/Execute Role
 - X86 Instruction Basics
 - Instruction Set Overview
 - General Purpose Instructions
 - Floating Point and SIMD Instructions
 - Program Flow Instructions
 - Hardware-Related Instructions
 - X86 Register Set Overview
 - General Purpose Registers (GPRs)
 - X87/MMX Registers
 - XMM/YMM/ZMM Registers
 - Segmentation Registers
 - Control Registers
 - Debug Registers
 - Model-Specific Registers (MSRs)
 - X86 CPU Operating Modes
 - Real Mode
 - Protected Mode
 - Virtual-8086 Mode
 - System-Management Mode (SMM)
 - IA32e (Long) Mode
- Platform Addressing
 - Introduction to x86 Address Spaces
 - Memory (DRAM and MMIO Space)
 - IO (Fixed and Relocatable Legacy Registers)
 - PCI (Peripheral Component Interconnect) Space
 - Platform Traffic Types
 - Programmed IO (PIO)
 - DMA (Direct Memory Access)
 - Peer-to-Peer
 - Memory Segmentation
 - Real Mode
 - Protected Mode
 - Memory Paging
 - Paging Basics
 - Translation Lookaside Buffer (TLB) Role
 - x86 Paging Modes: Basic 4K Paging, PSE, PAE, IA32e Mode Paging
- Core CPU Microarchitecture (10th Generation Ice Lake)
 - CPU Internal Architecture Overview
 - Instruction Pipeline & Execution Units
 - Instruction Fetch
 - Instruction Length Decoder (Predecode)
 - Branch Prediction
 - Instruction Queue
 - Decoders
 - uCode ROM
 - uOp Cache
 - uOp Queue and Loop Stream Decoder (LSD)
 - Allocate/Rename/Retire
 - Physical Register Files
 - Load and Store Buffers
 - Reorder Buffer (ROB)
 - Reservation Station (RS)
 - Execution Units
 - Implications of HyperThreading
- Architectural Differences: Cascade Lake Xeon Scalable CPU vs. Ice Lake Core CPU
 - Maximum Core/Thread Count = 28/56
 - Enhanced AVX Execution Unit Resources
 - 32KB L1 Code/Data Caches, 1MB L2 Unified Cache
 - Non-inclusive L3 Cache with 2D Mesh Interconnect
 - L3 Cache Slice Distributed Caching/Home Agent (CHA)
 - ECC DRAM and Support for Persistent Memory (Optane) PMDIMMs

- Cache Topics
 - Cache Basics
 - Five Memory Map Region Types: UC, WC, WB, WT, WP
 - Cache Policy Management: MTRRs and Paging Structures
 - CPU Conduct in the Five Memory Regions
 - Cache Hardware Architecture
 - Cache Ways and Set Associativity
 - Cache Directories and Tags
 - Least-Recently Used (LRU) Cache Line Tracking
 - L1 Cache VIPT (Virtually Indexed Physically Tagged) Scheme
 - Cache/Memory QoS and Intel Resource Director Technology (RDT)
 - Cache Monitoring Technology (CMT)
 - Cache Allocation Technology (CAT)
 - Code and Data Priority (CDP)
 - Memory Bandwidth Monitoring (MBM)
 - Other Cache Topics
 - PAT Feature
 - Software Prefetch Instruction
 - Non-Temporal Data
 - Data Direct IO (DDIO)
- Key Platform Interfaces
 - CPU and PCH Interface Overview
 - Main Memory DRAM
 - DRAM and DIMM Basics
 - Integrated Memory Controller (IMC)
 - DDR3 and DDR4 Differences
 - Row/Column Address Translation
 - Intel Ultra Path Interconnect (UPI)
 - Proprietary Intel Specification: Coherent CPU Socket Interconnect
 - 0, 2, or 3 UPIs per CPU, Up to 10.4 GT/s Each
 - Speed, Link PM, Packet Efficiency Improvements vs. QPI
 - PCI Express (PCIe)
 - Background
 - Key Features
 - Evolution: PCIe Gen 1 Through PCIe Gen 4
 - Universal Serial Bus (USB)
 - Background
 - Key Features
 - Evolution: USB 2.0 Through USB4
- PCI Configuration Space
 - Basics of Discovery and Enumeration
 - Client and Server Machine PCI Topology Examples
 - PCI Headers, Compatible Configuration Space, Extended Configuration Space
 - Accessing PCI Configuration Space
 - Arbor Software View of PCI Configuration Space
- Platform Interrupt Handling
 - Interrupt Background
 - The Controllers
 - Legacy 8259 PICs
 - IOAPIC
 - Local APICs
 - Message Signaled Interrupt (MSI/MSI-X) Basics
 - Interrupt Delivery and Remapping
 - CPU Interrupt Servicing

- Platform Power Management
 - ACPI Overview
 - CPU Power Management Features
 - Core & Device C-States, P-States
 - Power Management MSRs
 - Role of the Power Control Unit
 - Enhanced Intel Speed Step
 - Speed Shift
 - TurboBoost
 - PCH Power Management
 - Power Management Registers
 - Initiating Sleep State Transitions
 - Other PCH Power Management Features
 - IMC and DRAM Power Management
 - Integrated Memory Controller (IMC)
 - DRAM Power Management
- Platform Thermal Management
 - CPU Thermal Management Overview
 - TCC (Thermal Control Circuit)
 - DTS (Digital Thermal Sensors)
 - Thermal Management MSRs
 - Adaptive Thermal Monitor (ATM) and TM1/TM2
 - Thermal Interrupts
 - PCH Thermal Management
 - Thermal Sensors
 - Trip Points and Thermal Throttling
 - Reporting Thermal Data Over SMLink
 - DRAM Thermal Management
- System Management Mode (SMM)
 - SMM Background and Motivation
 - SMI and SMM entry
 - System Management Ram (SMRAM)
 - The CPU and PCH View of the SMRAM Address Range
 - SMI Delivery Considerations
 - Programming SMM Events
 - An SMM Example
- Machine Check Architecture (MCA)
 - CPU Error Types
 - The MCA MSR Register Sets
 - Machine Check Exception and Correctable Machine Check Interrupt (CMCI)
 - An MCA Error Logging Example
- Other Topics (Coverage Depends on Interest Level and Time Available)
 - Microcode Update
 - CPU Performance Monitoring
 - Virtualization Overview
- Appendices

Recommended Prerequisites: a basic understanding of computer architecture is very helpful

Course materials:

- 1) Course presentation PDF
- 2) [MindShare's "x86 Instruction Set Architecture"](#) eBook by Tom Shanley
- 3) Optional Add-On: [MindShare Arbor Software](#)
- 4) Optional Add-On: Intel Processor and Platform Architecture eLearning course