
intel
Leap ahead™
Intel Developer
FORUM

Benefits of Unified Extensible Firmware Interface* (UEFI) with Microsoft* and Other Operating Systems

Andy Liu
Software Development Manager, Software and Service Group, Intel Corporation

Yosi Govezensky
EFI Global Marketing Manager ,SSG, Intel

Session ID# SFIS003

Intel Developer FORUM

Legal Disclaimer

- INFORMATION IN THIS DOCUMENT IS PROVIDED IN 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.

- Intel and the Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
- *Other names and brands may be claimed as the property of others.
-

Agenda

- What Microsoft is saying about UEFI
- UEFI GPT breaks out of the 2 Terabyte limit
- Option ROM Size solution
- Boot Time enhancements
- OS Summary
- Demo

EFI Firmware
Great for the industry

- Standards-based
  - Well-specified and unambiguous
  - Conformance testing means cross-platform consistency
- Robustness
  - GPT support adds more fault tolerance
- Security
  - NVRAM entries to launch a boot option; no MBR bootstrap → no MBR Viruses
- Speed
  - Quicker hand-off from firmware to the Windows Boot Manager possible on Server systems
- Architecturally clean and modernized
- A native 64-bit firmware implementation for 64-bit processors
  - Take advantage of newer compilers and languages
- Eases bring up
  - Modular design speeds implementation bring up
- Eliminates BIOS complications
  - Eliminating the need for shadow memory enables more plug-in cards in a system
  - Server RAID option ROMs are very large and a single card may exhaust shadow memory
  - No 16-bit code

Standards Based

- UEFI Specification is controlled by the Unified EFI Forum (www.uefi.org)
  - AMI, Insyde, Phoenix
  - Apple, Dell, HP, IBM, Lenovo
  - AMD, Intel
  - Microsoft
- UEFI 2.0 is the current specification
- UEFI 2.1 is a work in progress

Agenda

- What Microsoft is saying about UEFI
- UEFI GPT breaks out of the 2 Terabyte limit
- Option ROM Size solution
- Boot Time enhancements
- OS Summary
- Demo

2 Terabyte Problem

0.75 Terabyte Drives
Shipping Today
Seagate Barracuda ES

terabyte	TB	2^{40} (10^{12})

RAID 0 with four
0.75 TB Drives
= 3 Terabyte Disk!

Legacy BIOS 2 Terabyte Problem

- The partition size of a bootable PC MBR disk must be smaller than 2 Terabytes.
  - The starting block and block size of a partition is a 32-bit sector address.
  - Sectors are assumed to be 512 bytes

$$2^{32} \times 2^{9} = 2^{41}$$

MBR Limitations

- Master Boot Record is the 1st 512 bytes of the hard driver
  - Contains 4 partition entries
  - Contains boot strap code
- More than 4 partitions are supported by encapsulating partitions in partitions
- Booting usually has to come from one of the 4 primary partitions
- Partition entry consists of
  - Boot flag – The 1st sector of the partition is loaded into memory by the code in the MBR and jumped to
  - LBA address of the partition 32-bit sector address
  - 32-bit size of the partition in sectors 32
- Since disks are traditionally made out of 512 byte sectors

MBR only address 2 Terabytes

EFI Solves 2 Terabyte Problem

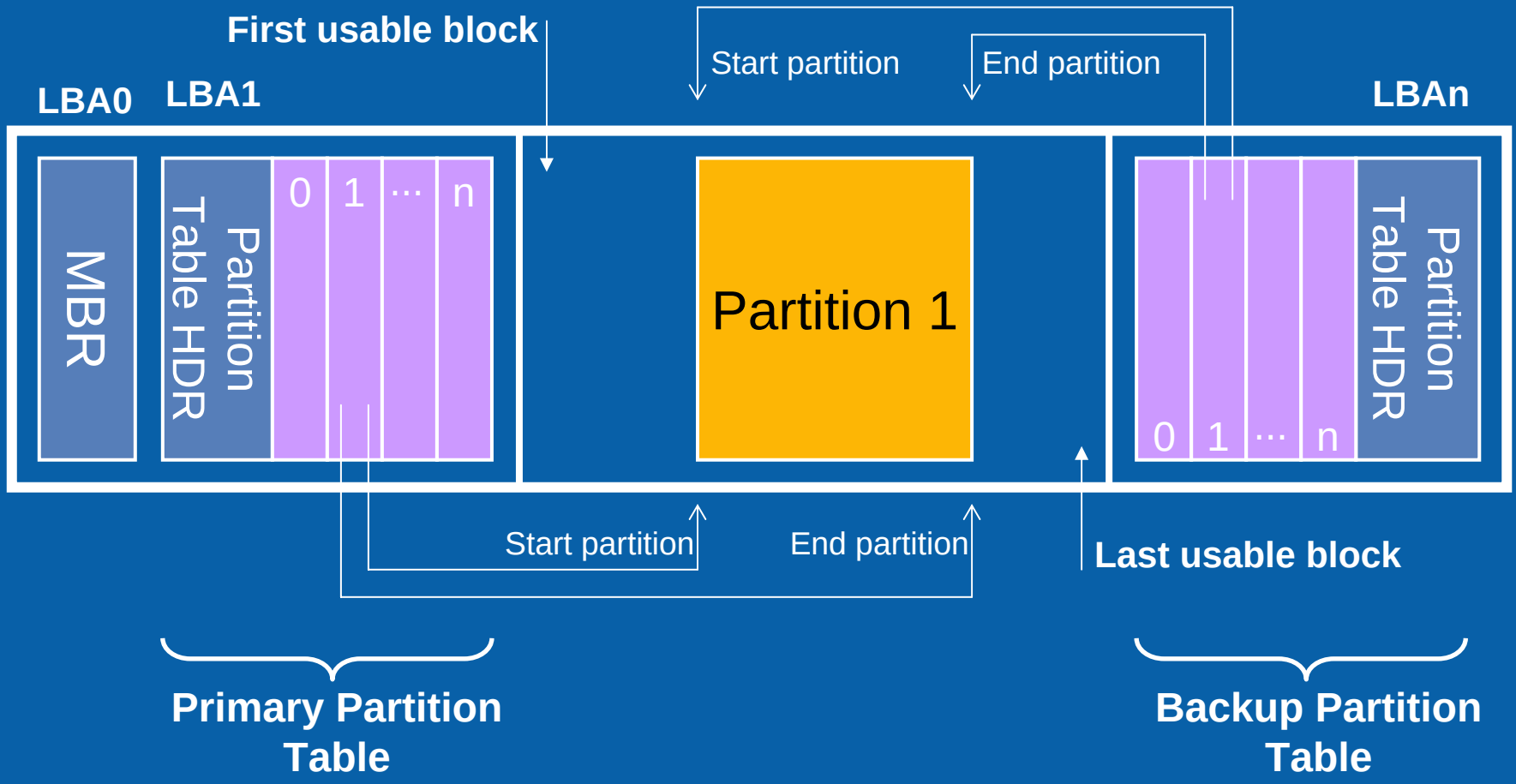
- EFI Solves the problem with GPT – GUID Partition Table
- A bootable EFI disk can be up to 2^{96} bytes.
  - A partition is described using a starting and ending 64-bit LBA.
  - Each LBA represents 2^{0} - 2^{32} of data. 512 bytes is the common block size for disks and 2048 bytes for CDs

$$2^{64} \times 2^{9} = 2^{73}$$

$$2^{64} \times 2^{32} = 2^{96}$$

1/16th Doggabyte? (2^{100} or 10^{30})

EFI GUID Partitioning Table



EFI GPT Features

- Every Disk has a unique GUID (128-bit unique serial number)
- Every partition has a unique GUID
- Each partition type has a GUID
- Unlimited number of partitions supported
- Partition table is replicated for better fault tolerance
- No magic code must execute as part of booting
- Fixes the 2 Terabyte Problem

Agenda

- What Microsoft is saying about UEFI
- UEFI GPT breaks out of the 2 Terabyte limit
- Option ROM Size solution
- Boot Time enhancements
- OS Summary
- Demo

Legacy Option ROM Challenges

- Option ROMs are more ISA oriented than PCI
  - 16-bit Real Mode Code
  - Limited Option ROM space (128K –192K)
- Size constraints lead to overly aggressive assumptions about what devices the ROM should manage
  - Onboard and plug devices may look similar to a plug-in ROM.
- Option ROMs need to slow down boot to place a hot key for configuration
- PCI Firmware Specification 3.0 confirms the issues
  - Adds device lists, DMTF CLP, execution above 1MB for configuration, but not runtime
  - Configuration is still confusing as Legacy, Hybrid, and delayed execution are all legal for ROMs and Systems

UEFI Option ROM Enhancements

- UEFI “Option ROMs” can be any where in system memory
  - No need to restrict the number of Option ROMs shadowed
  - Default is to let the ROM on the card manage the device
- UEFI allows platform to control policy
  - EFI_PLATFORM_DRIVER_OVERRIDE API lets platform control what Option ROM controls what device
- UEFI supports Option ROMs to register a configuration interface
  - Setup screen can take use of driver configuration protocol
- UEFI ROMs easy to implement by OS device driver writers

Option ROM Demo

2 systems
1 legacy and 1 EFI
Legacy System will Fail to boot

Agenda

- What Microsoft is saying about UEFI
- UEFI GPT breaks out of the 2 Terabyte limit
- Option ROM Size solution
- Boot Time enhancements
- OS Summary
- Demo

Legacy BIOS Boot Challenges

- Boot Device is magic A: or C:
  - C: is not deterministic, it is a function of boot sequence, although BBS spec can help
- BIOS boots via 512 bytes boot sector
  - Boot sector includes partition table
  - This code boots the next thing – loads the first 512 bytes of the partition
- A disk is limited to 4 root partitions
  - You can nest partitions inside of a partition
- BIOS needs to initialize most system devices for compatibility

EFI Advances Booting Technology

- EFI boots from a file on the media
- Boot file can be any size
- Deterministic and unique boot device
  - EFI Device Path protocol
- A disk can support a large number of boot options
- EFI boot media is backwards compatible with PC boot media
  - Media can boot legacy and EFI at the same time
- EFI by default only initialized devices needed to boot

Boot Time Demo

- Legacy system versus UEFI
- 2 Blackford Chipset based systems

  (1)UEFI Firmware

  (2)Legacy BIOS
- Boot to Microsoft x64 Longhorn

Agenda

- What Microsoft is saying about UEFI
- UEFI GPT breaks out of the 2 Terabyte limit
- Option ROM Size solution
- Boot Time enhancements
- OS Summary
- Demo

Microsoft Update

- Microsoft is targeting support of X64 and IA64 UEFI boot for Windows Server Longhorn
  - Coincides with the timeframe when heterogeneous mix of production quality UEFI firmware should be available for broad based consumption
  - EFI 1.10 support continues for current IA64 systems
- UEFI members should attend UEFI Plugfest in Dec
  - Microsoft will be there to test your implementations
  - If not a member JOIN!! And attend the plugfest
  - Details at www.UEFI.org

EFI Firmware "Great for the industry"

Linux Update

- EFI Itanium® Processor booting has been supported for many years
- Current IA32 EFI OS versions shipping
  - Red Flag Linux
  - EFI interfaces checked in since Kernel 2.6.1
  - ELILO created as EFI boot loader on Sourceforge
- Work in progress on updating to UEFI 2.0
  - Kernel updates to UEFI 2.0 x86-64
  - ELILO updates to UEFI 2.0 x86-64
  - Grub update to UEFI 2.0 x86-64
- Linux-ready Firmware Developer Kit supports EFI

Linux will support x86-64 UEFI

Apple iMac Demo

Break out of the PC Mindset

Together we can do more

- Itanium® Processor based platforms have been using EFI for years
- Apple is shipping millions of Intel EFI systems every quarter
- All major Operating System venders already / have a plan to support UEFI
- Join the Unified EFI Forum and help shape the future
- Join an open source project at www.TianoCore.org and contribute to the community
- Build innovative product plans around UEFI
  - IHV have compelling UEFI Option ROM
  - OEMs build innovative UEFI based platforms
  - ISV build interesting UEFI based solutions

Join the Leaders Implementing UEFI

Call to Action

- OEMs
  - Provide systems to Microsoft with UEFI (now)
  - Attend UEFI SCT plugfest event in Dec ’06
  - Download Vista/longhorn beta 2 or later and test/install UEFI X64
    - winboot@microsoft.com
- IHVs
  - Provide UEFI drivers for your boot related cards
    - Storage (atapi, sata, …)
    - Lan
    - Video
    - Input device (keyboard, mouse etc)
- ISVs
  - Write UEFI preboot programs
    - Installation, setup and testing
    - Disk utils, backup of disk and nvram storage
    - Virus scanning, system migration, setup/installation of cards

Summary

- EFI Firmware “Great for the industry”
- “Eliminate BIOS Complications”
- Break out of the PC Mindset
- Join the leaders implementing UEFI

UEFI Testing Event

- In Dupont, Washington State, US – Week of December 11
- Purpose
  - Provide the an opportunity to allow implementers of UEFI to test their implementations among the UEFI community
  - Testing of UEFI systems and platforms with UEFI add-in cards in different configurations for UEFI compliance as well
  - Testing install and boot to a variety of UEFI Operating systems
- Contact laurie.fleisher@intel.com
- More on this event: www.uefi.org

Your Opportunity to Test your Implementation

Intel Developer FORUM

Essential References and Resources

- Technical book from Intel Press:

  Beyond BIOS: Implementing the Unified Extensible Firmware Interface with Intel's Framework

  by Vincent Zimmer, Michael Rothman, and Robert Hale

  For more info: www.intel.com/intelpress

Additional EFI /Framework Sessions ShangHai 2006:

Session	EFI #	Company	Time
New Firmware Development at Hewlett Packard using EFI and the Framework	SFIS001	Hewlett Packard	Done
Mobile Platform Usage of UEFI and the Framework Technology	SFIS002	Intel Mobile	Done
Benefits of Unified Extensible Firmware Interface (UEFI) with Microsoft and Other OS	SFIS003	Intel	Done
Intel Advanced Technology in the Enterprise: UEFI Firmware & IBM	SFIS004	Intel	16:30

More web based info: www.TianoCore.org

www.uefi.org

www.intel.com/technology/framework

Please fill out the Session Evaluation Form.

Session presentation will be available on IDF web site – www.prcidf.com.cn

Thank You!

Backup Slides

Microsoft Information

- Hardware Design for Windows Vista
  - Firmware and Boot Environment
  - http://www.microsoft.com/whdc/system/platform/firmware/default.mspx