Intel – Trusted Platforms Overview

Greg Clifton
Intel Customer Solutions Group
Director, DoD & Intelligence

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.
-

Intel® Platforms

Business Desktop	• Built-in Manageability • Proactive Security • Energy Efficient Performance
Digital Home	• Performance • Energy Efficient • Connectivity • Ease of Use
Mobility	• Performance • Battery Life • Uncompromised Connectivity • Innovative Form Factor
Server	• Effective Virtualization • Optimized Power & Thermals • Reliable Data Intensive Computing

Agenda:

- It is an imperfect world
- Building the foundation in 2006
- The 2007 “Weybridge” Platform
- Solving the problems with Intel vPro™ technology
- Conclusions

Energy Efficient Performance

Today's Challenges

- Managing and Securing modern business clients is more challenging than ever
  - Zero day malicious exploits create scenarios that patching alone can't resolve
  - Layered security improves platform protection capabilities
  - Optimized platform architecture removes bottlenecks, but also introduces complexity
  - Damaged software or hardware can impair the ability to remotely repair a client

- Client PCs are not manageable when they need it most, i.e. HW or SW problem or turned "off".
  1. Desk-side visits & manual processes drive disproportionate share of IT costs
  - Intel IT: ~10-15% of help desk calls require desk-side visit, but drive ~50% of help desk costs
  2. Security threats increasing, time to respond decreasing but protections vulnerable to attack or user tampering
  - Time to exploit = 3 days; Time to vendor patch = 42 days

No single technology solves all of these problems!!

Intel's Platform Solution

- Utilize a set of technologies that work together to:
  - Enable innovative solutions to solve these problems
  - Create a new framework for a rich layered security architecture

Evolving Intel® vPro™ in 2007 – "Weybridge"

Intel Core™ 2 Duo

Bearlake Family Chipsets

Wolfdale CPU Support

Intel Trusted Execution Technology™

Windows Vista* Premium Logo

Intel® Active Management Technology 3.0

2007 Weybridge Platform

eSATA*, Expanded USB*, Intel® Rapid Recovery Technology

Enhanced Virtualization (VTd)

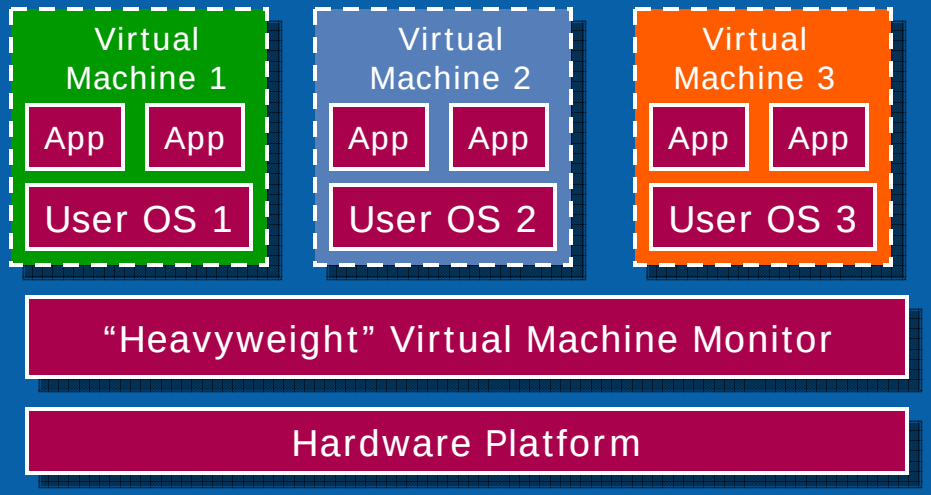
Reduced Chipset & Platform Power

Note: Certain features may be available only on particular SKUs

*Other names and brands may be claimed as the property of others

Intel® Virtualization Technology

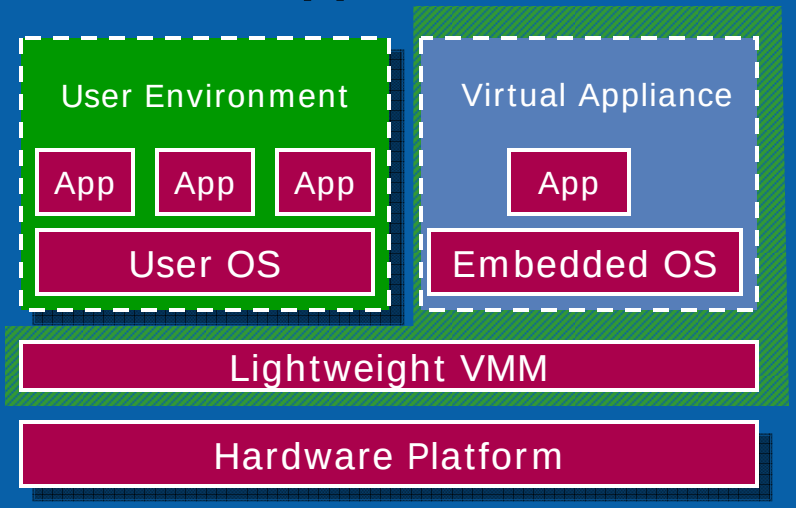
Traditional Virtualization



Full OS Partitions

- Full OS capability
- Multiple applications
- Full HW suite available
- Generally virtualized devices
- Maximum features and capability agility

Virtual Appliance Model

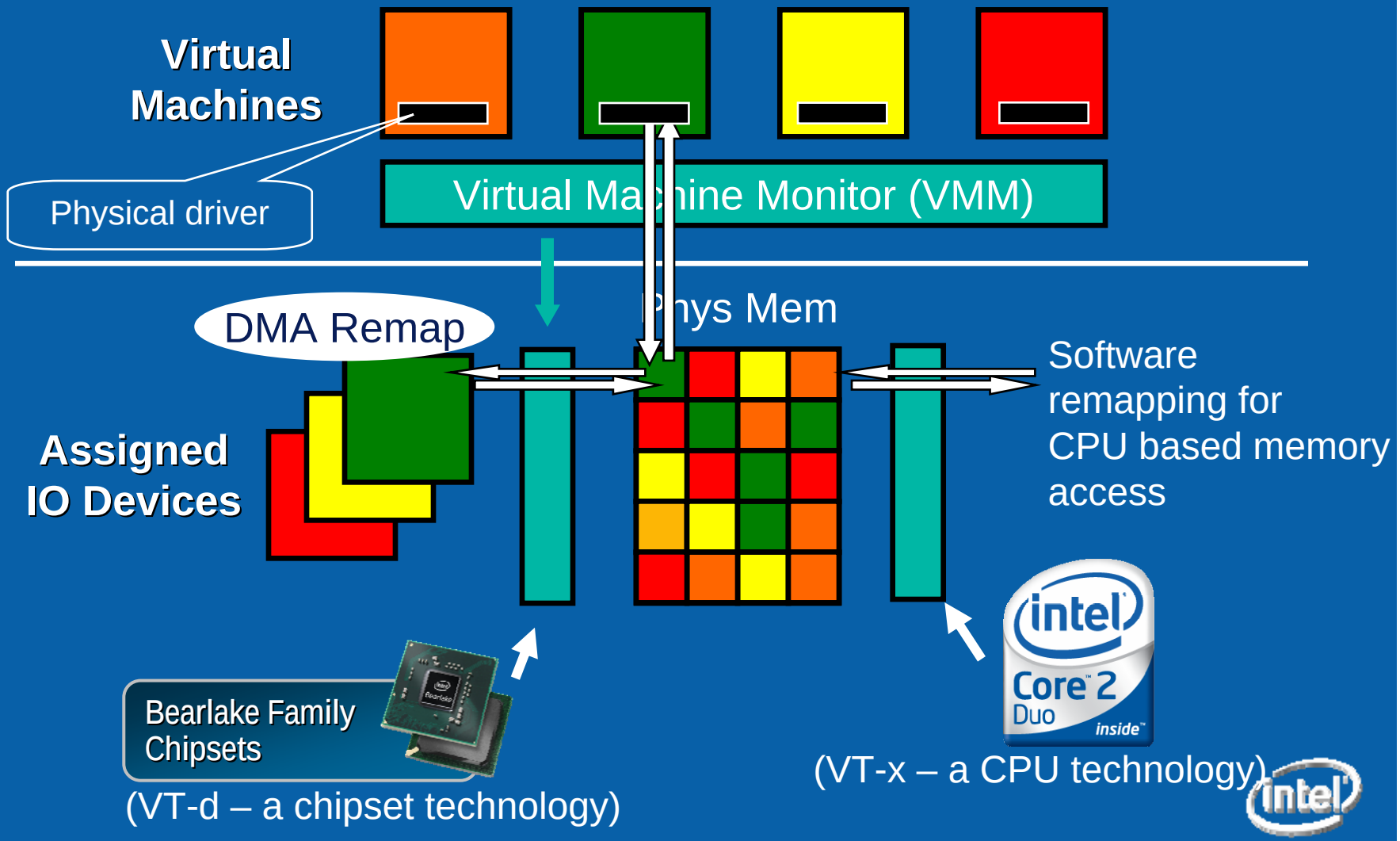


Virtual Appliance Partitions

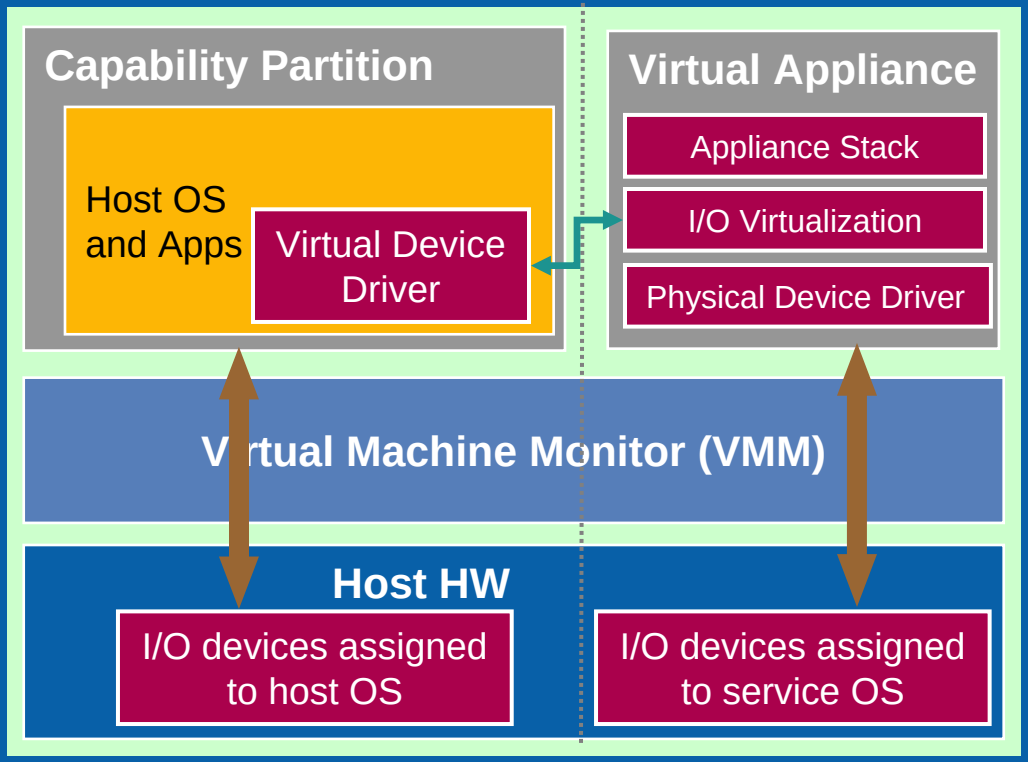
- Generally headless
- Fixed/specific function
- Low OS profile
- Minimal management cost
- Minimal platform resource utilization
- Minimal true/virtual HW mapped
- OS state/power independent

Make Virtualization Applicable to Mainstream

VT-d Direct I/O Overview



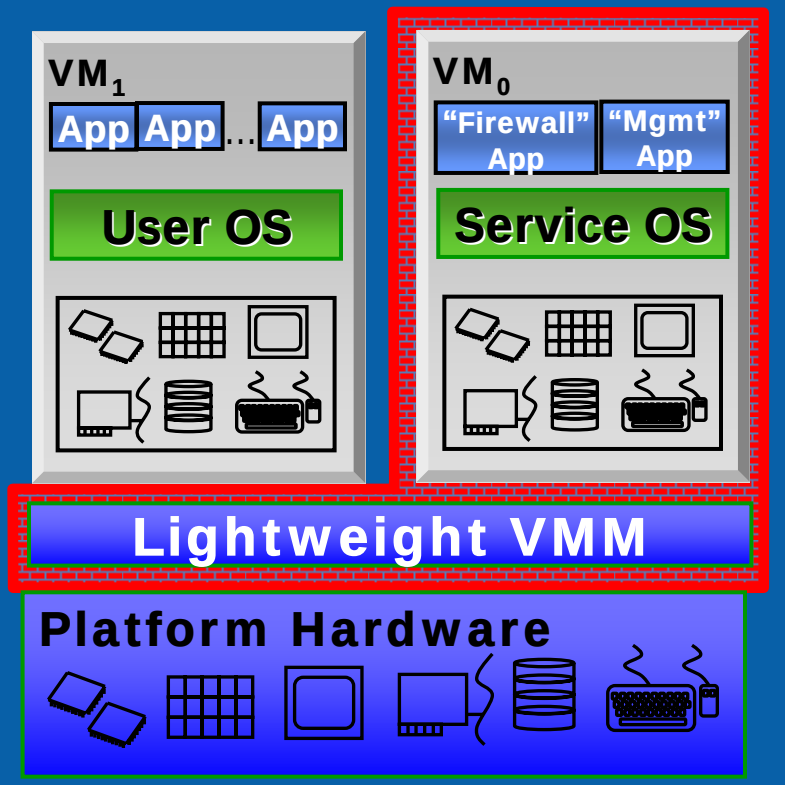
VT-d : DMA based Protection and Remapping for Virtual Appliances



- VT-d enables
  - Flexible memory management by VMM
  - Un-modified device drivers to run in both partitions
  - Contain DMA errors across partitions
  - Allows enforcement of independent security policies for each partition

Intel Trusted Execution Technology™ Introduced on Weybridge for Increased Security

- Codename LT extends Intel® VT capabilities of partitions and isolation to increase security using
  - Measured launch and a chain of trust to generate a secure partition
  - Trusted Platform Module (TPM) for Secure Storage of measurements and Signed reporting



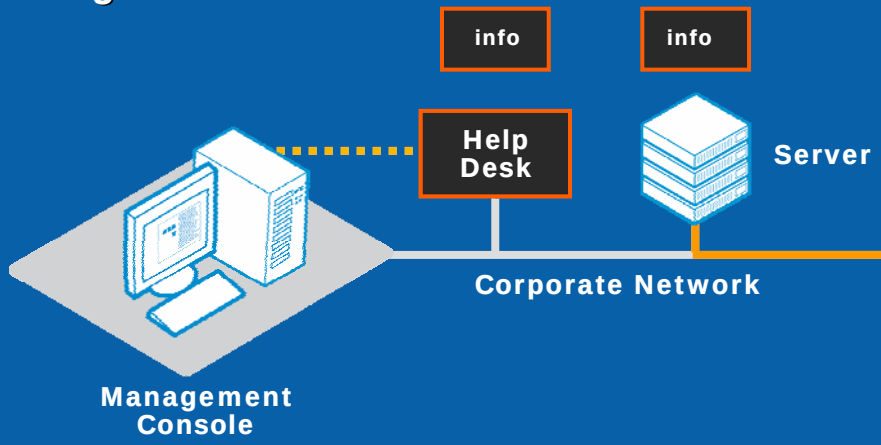
Intel® Active Management Technology Overview

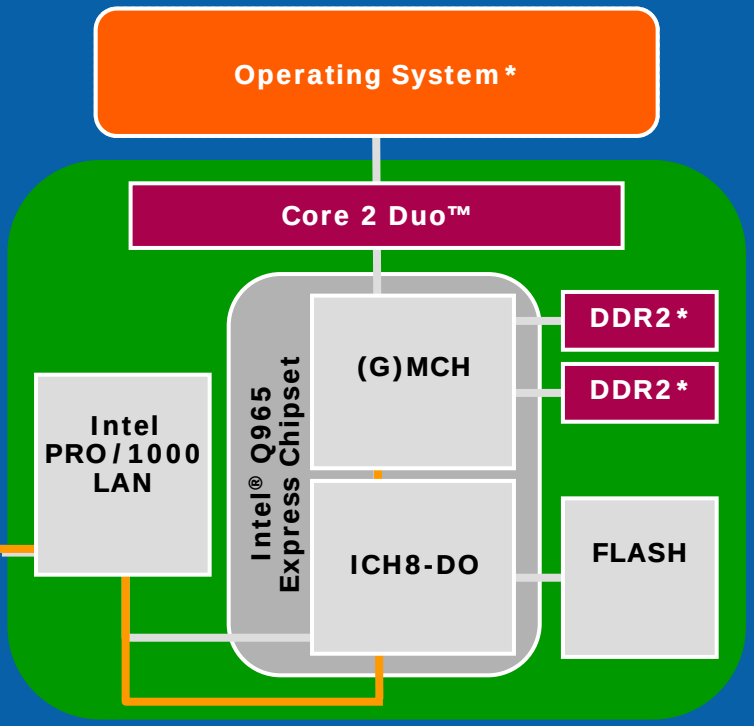
- Provides Built-in Manageability and Proactive Security for networked computing resources
- Enables maintenance and repair of systems using out-of-band
  (OOB) management capabilities even if the system is powered
  off or the OS is down
- Helps secure networks by:
  - Proactively blocking incoming threats
  - Reactively containing the spread of threats
  - Ensuring critical software agents are present
  - Keeping installed software versions up to date
  - Enabling popular third-party management consoles and security applications in use today

[1] Intel® Active Management Technology requires the platform to have an Intel® AMT-enabled chipset, network hardware and software, connection with a power source, and a network connection.

Intel® AMT 06 Architecture Overview

- **Discover**
  - Enhanced non-volatile memory storage
  - Out of Band access
- **Heal**
  - Provisioning & remote control
  - Hardware Diagnostics
- **Protect – System Defense: Filtering features**
  - Capability to allow, disallow, rate-limit packets based on 5-tuple IP Protocol Filter
  - Filters programmed by remote console
  - Filtering in hardware for LAN
  - Agent Presence

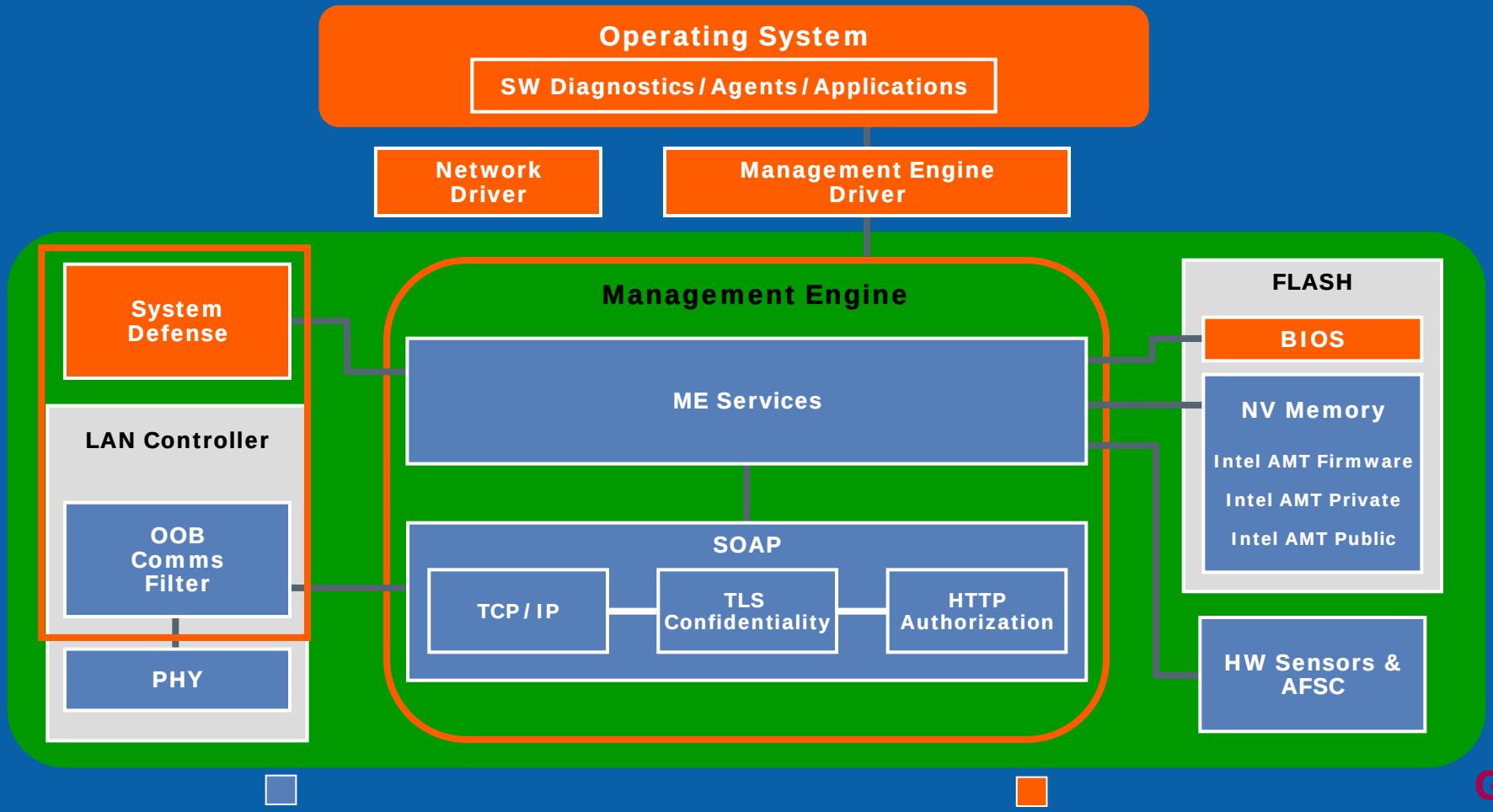




Intel® Active Management Technology

Major Intel® AMT Components

OOB Communication, Management Engine, Nonvolatile Memory



Go

Intel® Active Management Technology
Usage Cases

- Remote Asset Inventory
- Hardware and Software Inventory
- Remote Diagnostics and Repair
- Encrypted, Remote Power-on and Update
- Agent Presence Checking
- Hardware-based Isolation and Recovery

Intel® AMT Core Attributes
Advantage over S/W Solutions

- **OS and HDD-Independent**
  - Runs outside the context of the OS
  - Works the same way regardless of the installed OS
  - Immune from OS configuration issues
- **Highly-Available OOB Remote Management**
  - Provides remote management capabilities in all system power and health states
  - Runs on auxiliary and battery power (mobile)
  - Wired and wireless network support (2007)
- **Tamper-Resistance**
  - Intel® AMT agent bound to the PC and configured by IT
  - Resistant to end-user modify/disable
  - Network and Host I/F Security

Intel AMT Capabilities

Advantage over H/W (WoL & ASF) Solutions

Capabilities	WoL	ASF 2.0	Intel® AMT
OOB Mgt (Any OS/power state)	Booting Only	Boot/reboot and alerts	Boot/reboot, alerts, event log, and remote control, redirection
Remote Control	Remote Boot Only	Remote Boot/Reboot w/boot options	Remote boot/reboot w/ boot options, Serial Over LAN, IDE redirection
Event Alerting	No	Yes (1 Client, no filtering)	Yes (Broadcast to 16 clients, filter only desired events)
3rd Party Non-Volatile Storage	No	No	Yes
Event Logging	No	No	Yes, including filters
Remote Reboot	No	Yes (PXE)	Yes (PXE or IDE-Redirect)
Asset Information	No	No	Yes
Remote BIOS Update	No	No	Yes
Secure Communications	No	Simple authentication - no encryption	SSL 3.1/TLS encryption, HTTP Digest/Negotiate authentication
Connection Protocol	None	RMCP	SOAP/HTTP (web browser access)
Layer 4 Stack	Registered packet	UDP	TCP (preferred routing protocol)
Firmware Updates Utility	No	No	Yes
System Defense / Agent Presence	No	No	Yes
System Defense /NOC Filters	No	No	Yes

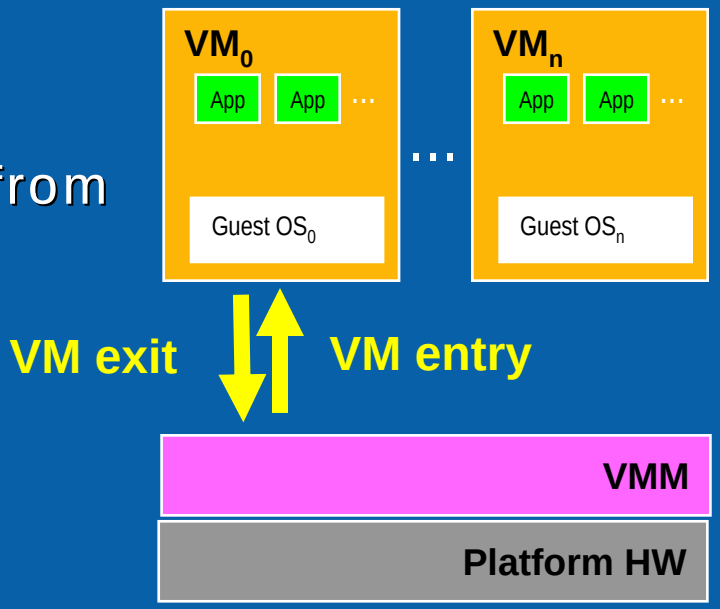
Conclusion

- Solving yesterday's problems with enhancements to yesterday's solutions is not sufficient to address the challenges of tomorrow
- We are well underway to redefining the PC
  - Radical new hardware that enables distinct technologies that work together being launched in 2006 and 2007
  - New class of solutions that solve problems in new ways are starting to emerge
  - Barriers to innovation are being cleared for ISVs
  - This is just the beginning – new innovations to come for the 2008 platform and beyond– stay tuned…


intel
Leap ahead™

Intel® Virtualization Technology Mode Transitions

- VM entry (VMLAUNCH/VMRESUME)
  - Transition VMM ➔ Guest
  - Enters VMX non-root operation
  - Loads Guest state and Exit criteria from VMCS
- VM exit (VMEXIT)
  - Transition Guest ➔ VMM
  - Enters VMX root operation
  - Saves Guest state in VMCS
  - Loads VMM state from VMCS
  - May be triggered by many causes
    - E.g. Accessing CPU MSRs



Intel® Virtualization Technology Operation with VMCS