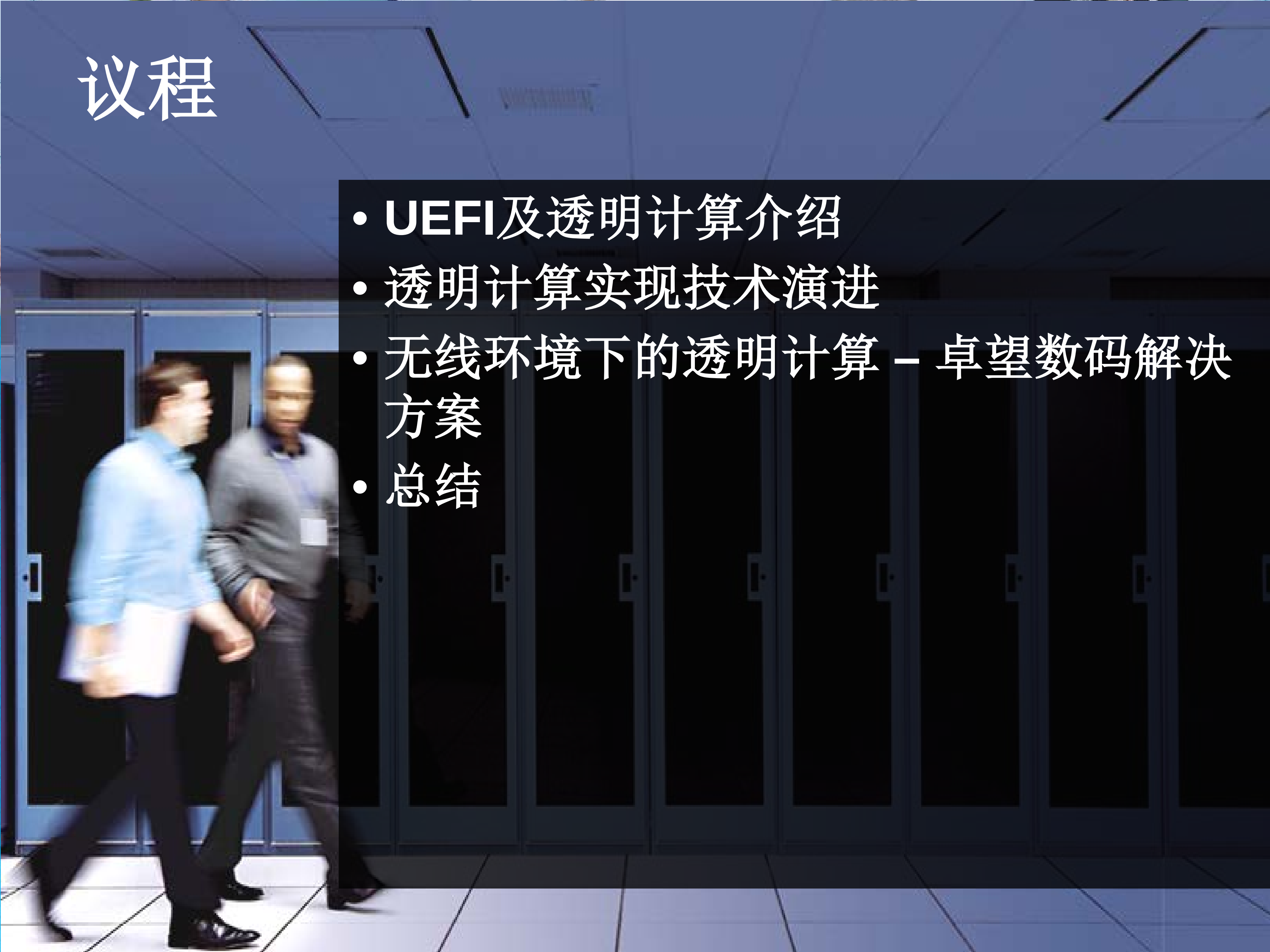
# UEFI 和透明计算技术

吴铭 UEFI嵌入式开发部经理
英特尔软件事业部
刘克鸿 首席架构师
卓望数码

EFIS003

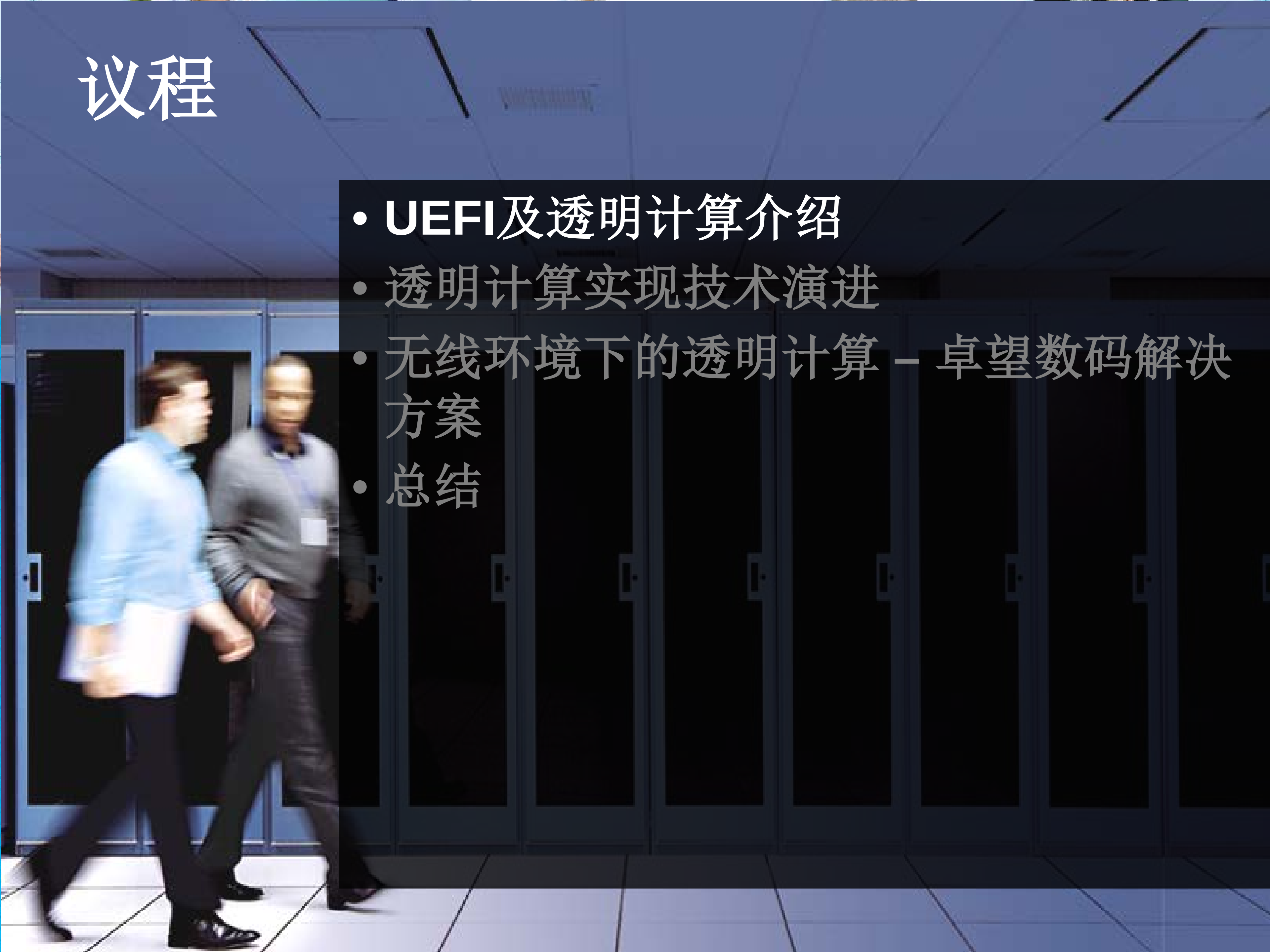
英特尔®与你共创明天™

# 议程



- UEFI及透明计算介绍
- 透明计算实现技术演进
- 无线环境下的透明计算 – 卓望数码解决方案
- 总结

# 议程



- UEFI及透明计算介绍
- 透明计算实现技术演进
- 无线环境下的透明计算 – 卓望数码解决方案
- 总结

# BIOS到UEFI的转换

**2000之前**

所有BIOS都是封闭的

**2000**

英特尔发明可扩展固件接口(EFI) 并以BSD License的方式公开其参考实现

**2004**

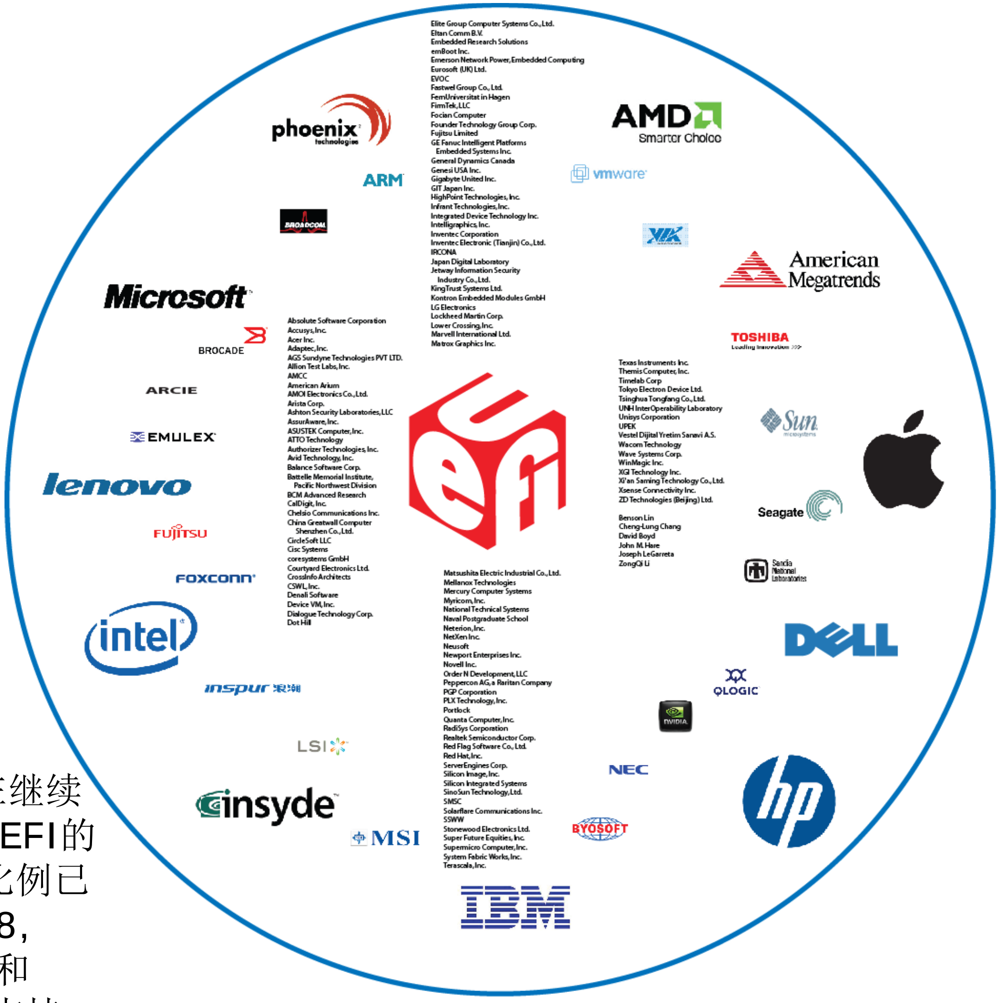
**tianocore.org - 开源**EFI社区发布

**2005**

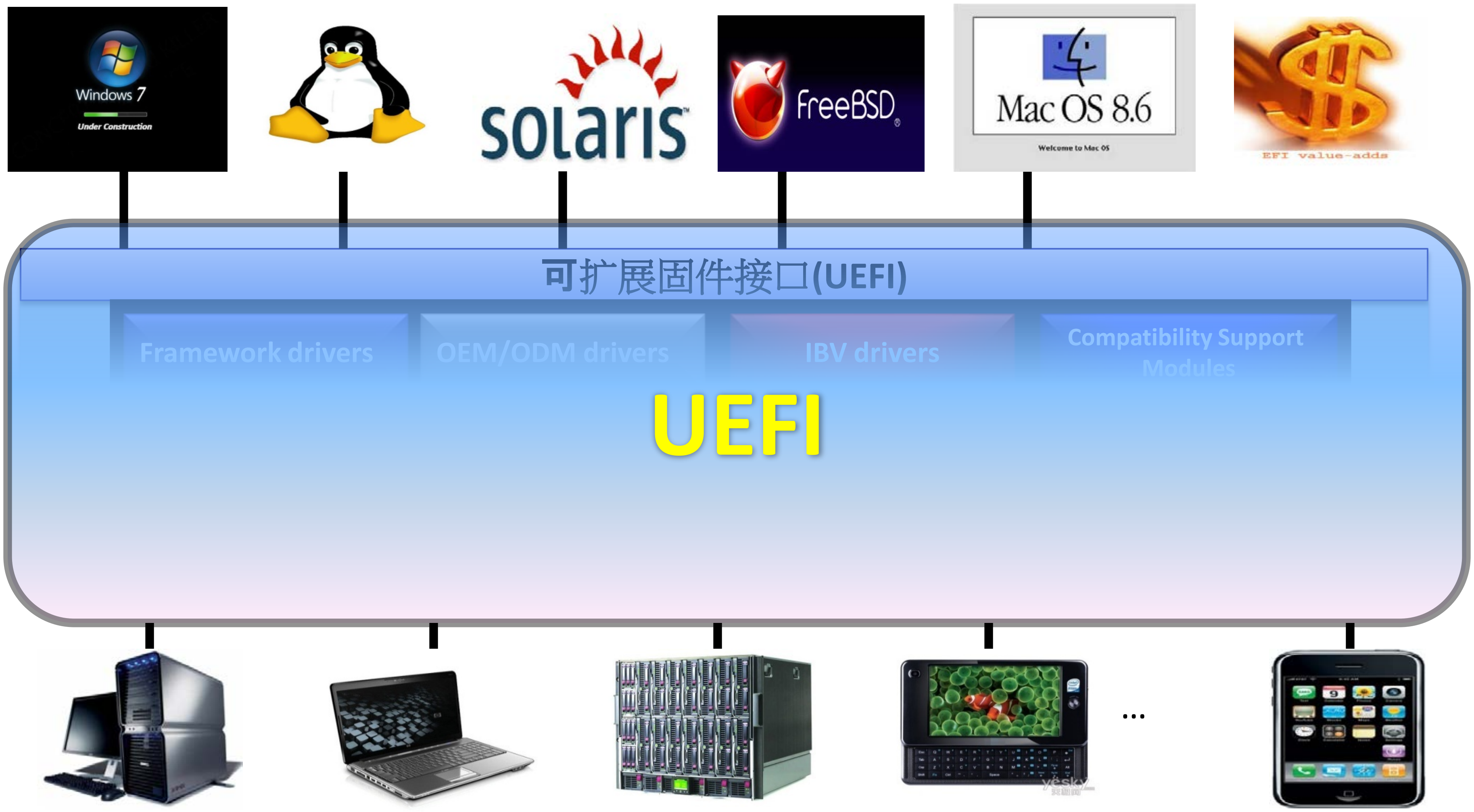
与11家业界成员共同发起UEFI (Unified EFI)论坛，致力于EFI的标准化工作

**2011**

UEFI成员数已达170并且还在继续增长，主流MNC都已发售带UEFI的产品，全球所有IA产品UEFI比例已超50%，微软的Server 2008, Vista*及Win7*，RedHat* 和Novell*的操作系统产品都已支持UEFI x64



# UEFI 抽象硬件平台



可扩展固件接口(UEFI)

Framework drivers

OEM/ODM drivers

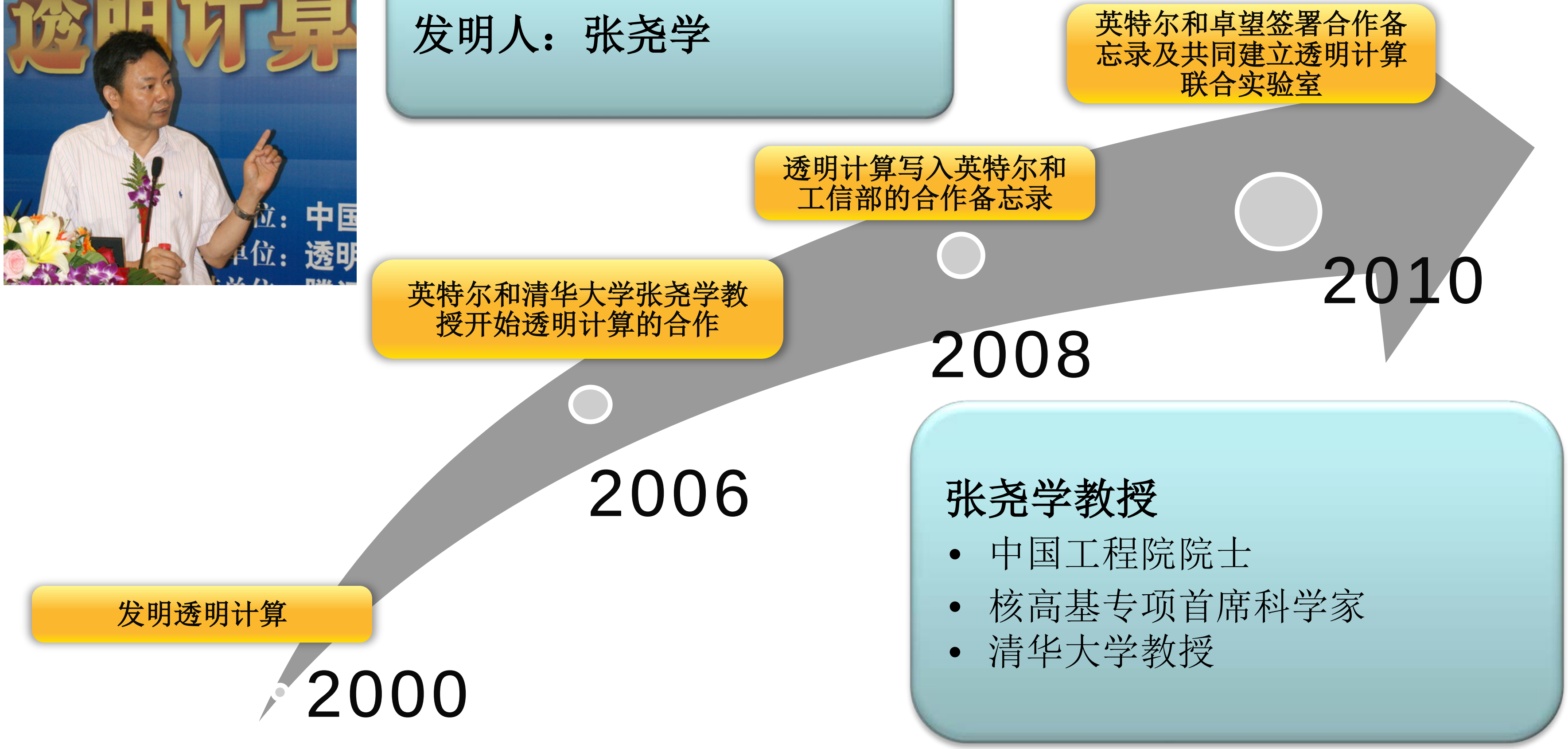
IBV drivers

Compatibility Support Modules

UEFI

# 透明计算历史

发明人：张尧学


2000

发明透明计算

2006

英特尔和清华大学张尧学教授开始透明计算的合作

2008

透明计算写入英特尔和工信部的合作备忘录

2010

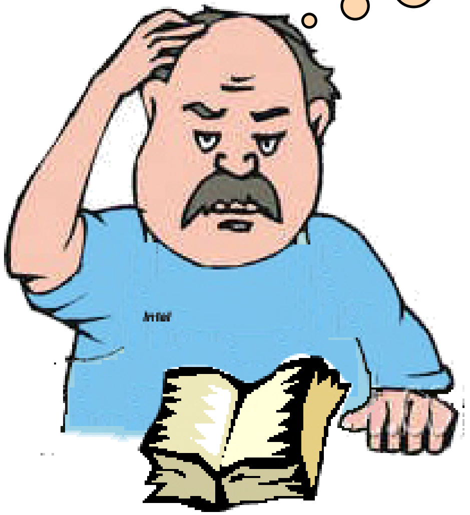
英特尔和卓望签署合作备忘录及共同建立透明计算联合实验室

**张尧学教授**

- 中国工程院院士
- 核高基专项首席科学家
- 清华大学教授

*目标：计算无处不在*

# 透明计算的起源



思考：如何象看电视一样方便地使用计算机？

## 电视机

即开即看
只关注内容，不关注机器维护
易于升级

## 计算机

硬盘格式化、安装操作系统、系统配置、应用程序管理、杀毒、备份…
升级系统时需要重复上述步骤

## 根源：计算机终端过于复杂

终端集成了太多的软件，而绝大多数平时都不用

## 未来计算机

即开即用
最终用户只关注内容
与平台无关，易于升级

IDF2011
英特尔信息技术峰会

# 透明计算

## 希望解决的问题

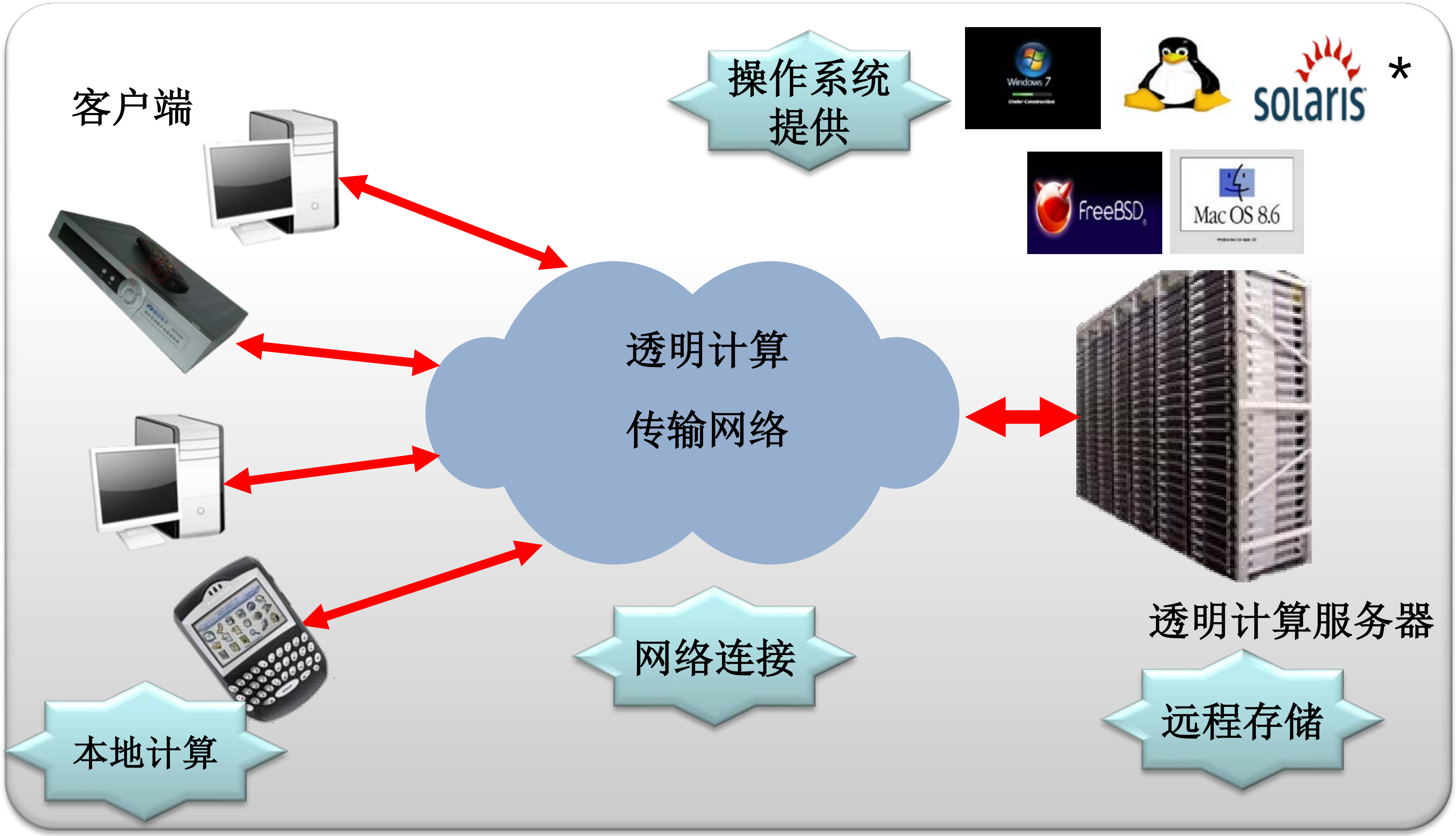
- 计算机终端运行更高效
- 存储更有效
- 安全、可管理、低成本
- 从面向设备到面向用户的转变
- 软件即服务

## 如何解决这些问题?

- 软件硬件逻辑分离
- 计算存储分离
- 软件即服务
- 网络提供服务

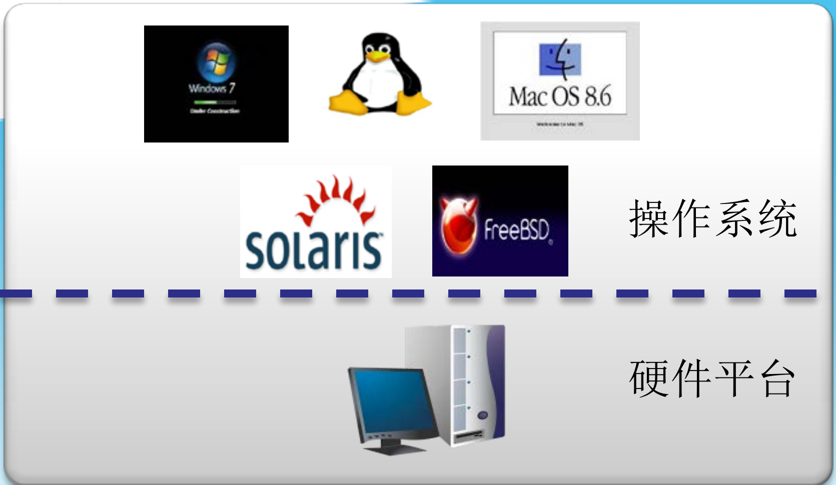
***抽象磁盘I / O网络重定向***

# 透明计算概念


客户端
操作系统
提供
Windows 7
solaris
*
FreeBSD
Mac OS 8.6
透明计算
传输网络
透明计算服务器
网络连接
远程存储
本地计算

# 典型用户场景

## 相同硬件不同软件



操作系统

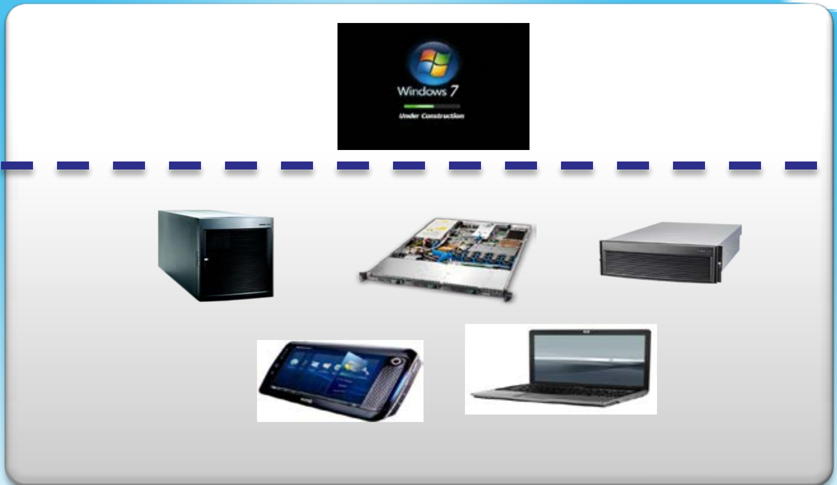
硬件平台

教育

银行

呼叫中心

## 相同软件不同硬件



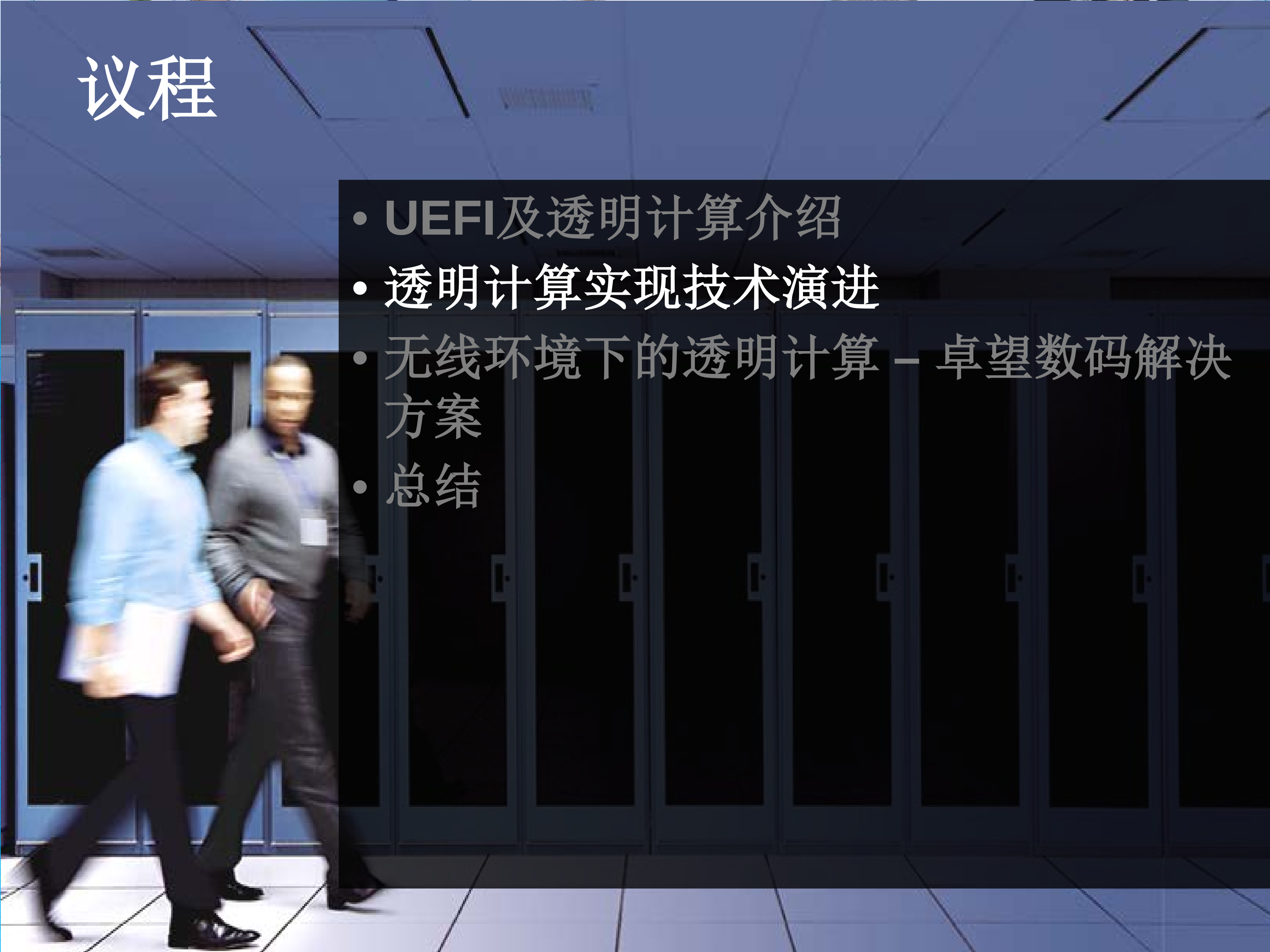
远程办公

服务运营

移动运营商

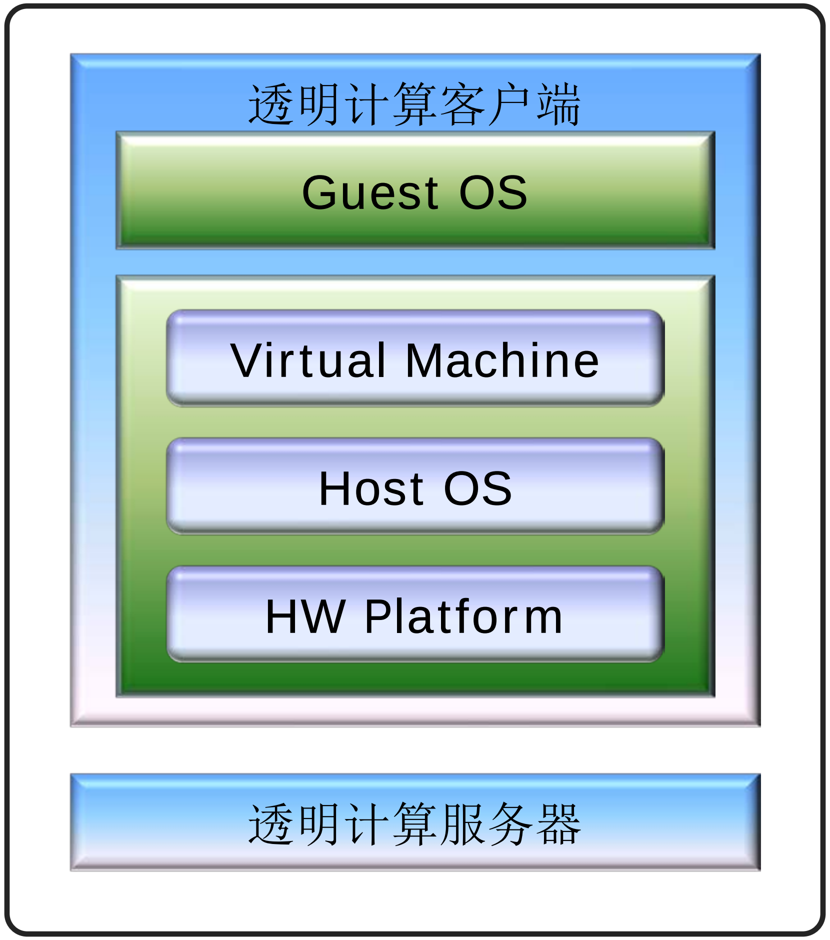
***软件硬件逻辑分离***

# 议程



- UEFI及透明计算介绍
- 透明计算实现技术演进
- 无线环境下的透明计算 – 卓望数码解决方案
- 总结

# 透明计算技术演进 – 全虚拟

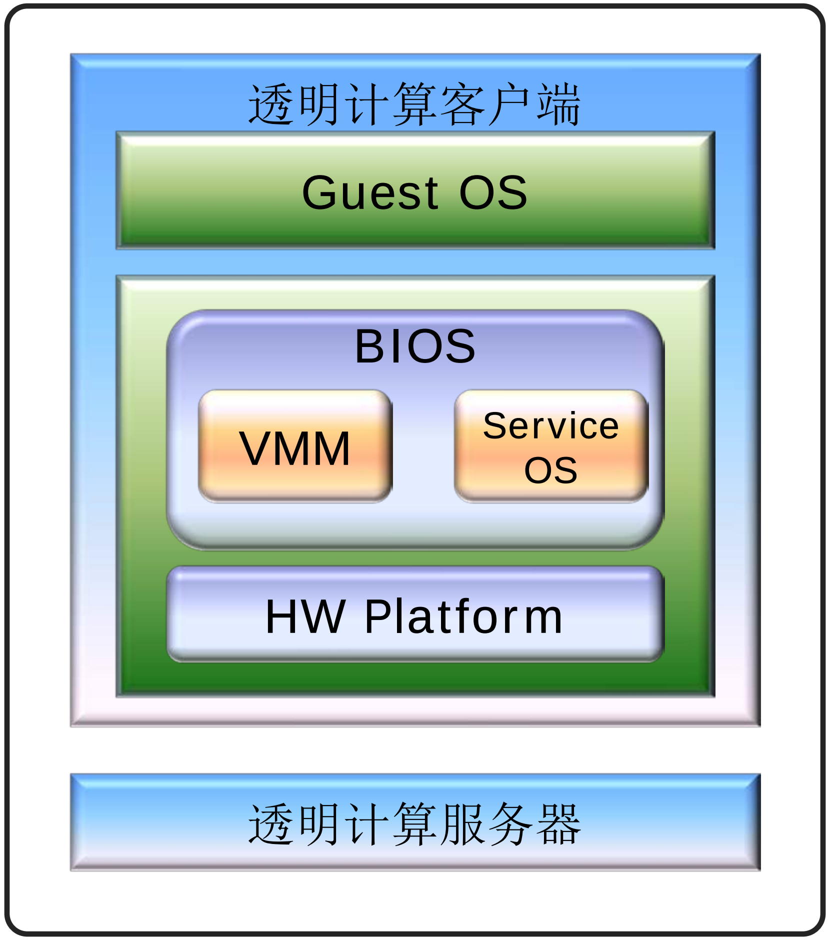


## 要点

- Guest OS运行于虚拟机之上
- 将嵌入式Linux嵌入BIOS作为Service OS
- VMM运行于Linux之上

| 优点 | 局限 |
|---|---|
| 与硬件无关<br>支持所有操作系统<br>完全透明 | 性能比较低 |

# 透明计算技术演进 – 部分虚拟



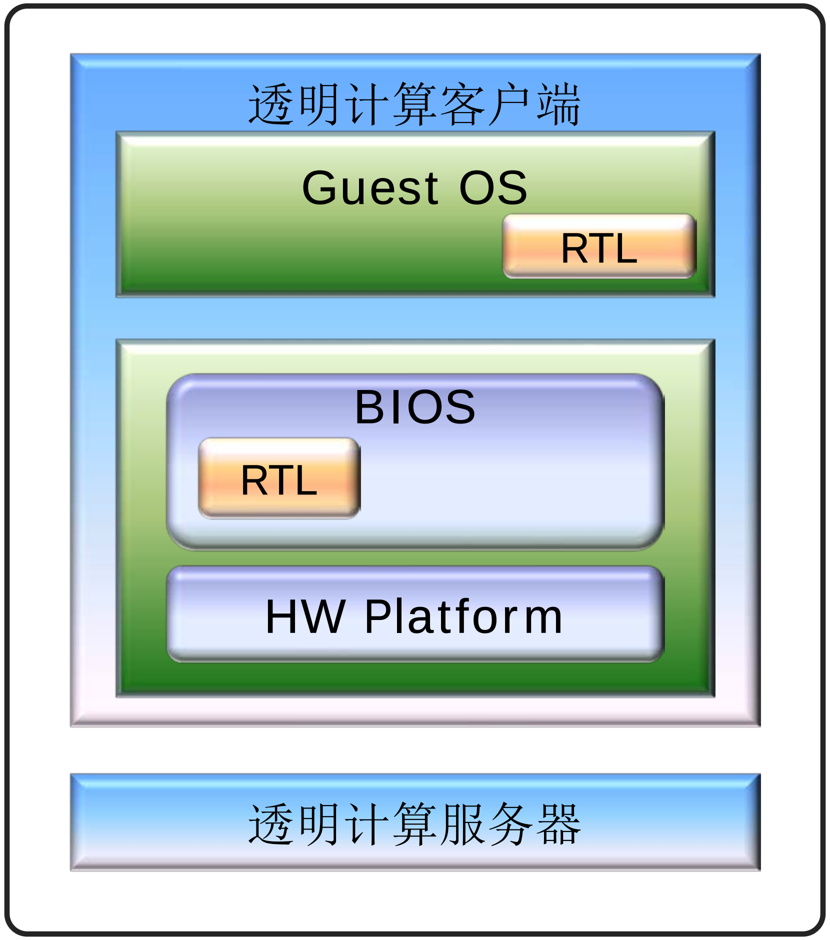
## 要点

- VMM截获IDE和网卡的访问并将磁盘块IO重定向到Service OS
- Service OS将磁盘块IO通过网络重定向到远程
- 其他设备的IO操作由硬件直接处理

| 优势 | 局限 |
|---|---|
| 性能显著提升<br>基本透明<br>不需要修改操作系统 | 硬件平台需要支持VT |

IDF2011
英特尔信息技术峰会

# 透明计算技术演进 – 非虚拟技术



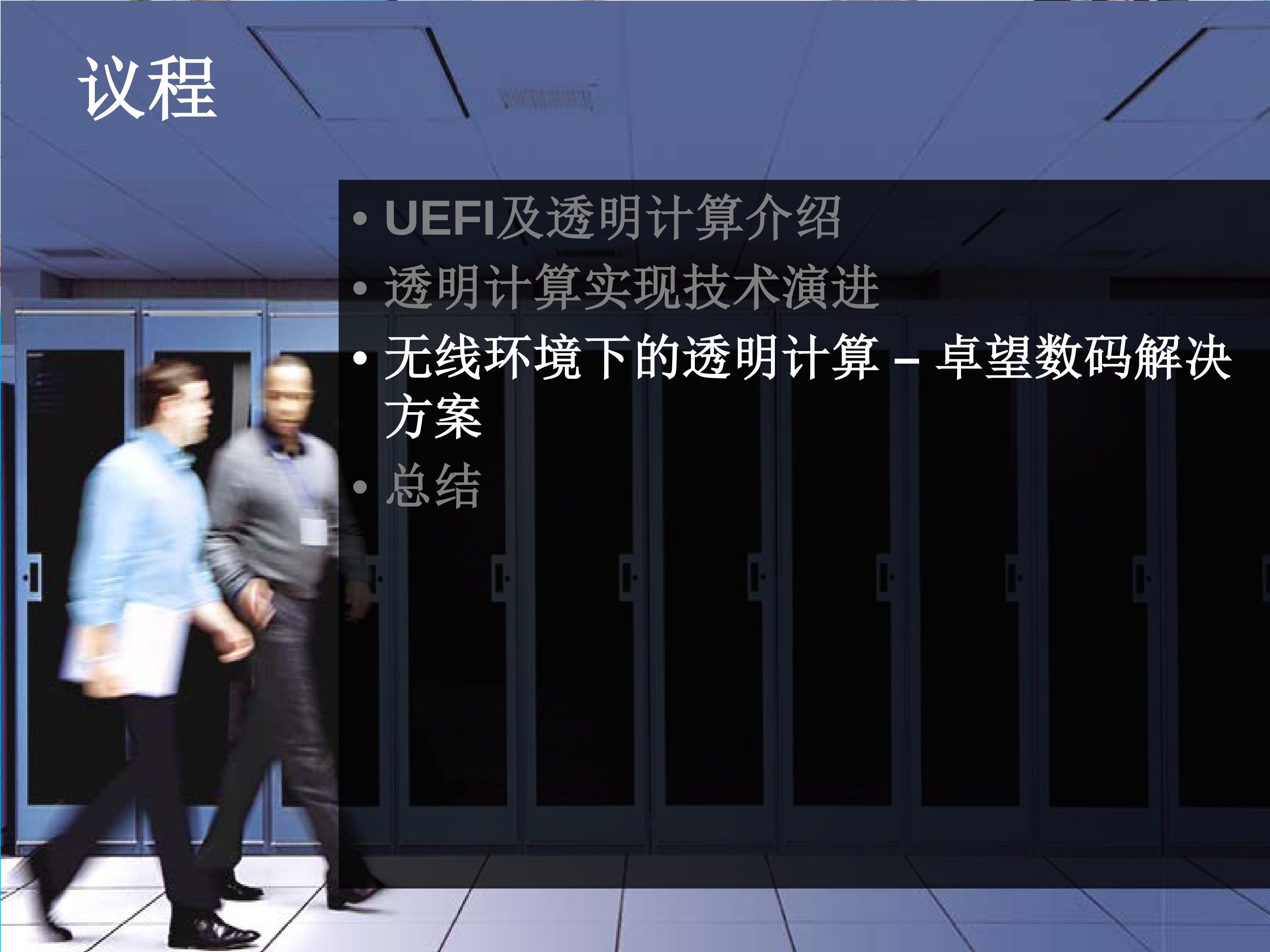
## 要点

- 在BIOS内截获boot-loader的磁盘读写IO
- 在操作系统内截获OS的磁盘读写IO
- 重定向磁盘读写IO到远程

| 优势 | 局限 |
|---|---|
| **性能高**<br>**不依赖于硬件** | **操作系统需要修改和移植，有一定的开发量** |

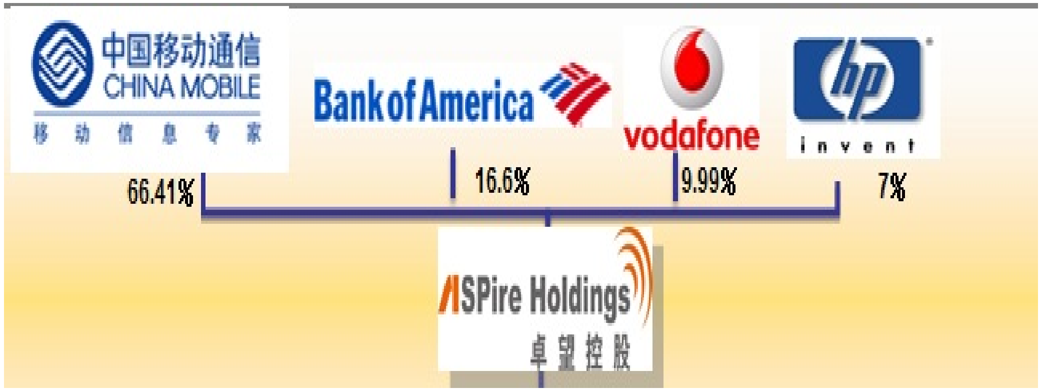
RTL：Resource Translation Layer，资源转换层

# 议程



- UEFI及透明计算介绍
- 透明计算实现技术演进
- 无线环境下的透明计算 – 卓望数码解决方案
- 总结

# 卓望公司介绍



- 成立于2000年
- 约3000员工
- 为中移动、 新加坡电信, Starhub, 澳大利亚电信及中移动香港提供数据服务、互联网服务开发与运营
- 国家级高新技术企业
- 国家级核心软件企业

# 卓望 / 中移动项目需求

便携无线终端

性能功耗比
支持电话功能

软件即服务

运营商以软件提供的方式提供增值服务
系统补丁，比如安全包

中国移动通信
CHINA MOBILE

中移动典型应用

PINM（个人信息网络管理）
高清照片即拍即传
视频会议

专用市场

支持windows操作系统
易于第三方厂家的软件开发

# 移动计算面临的问题

## 移动计算问题（容量6亿的大用户市场）

- 移动设备的病毒威胁
- 恶意软件
- 高端设备不利于市场推广
- 终端丢失所造成的信息丢失
- 升级困难
- 应用软件冲突
- 网络流量

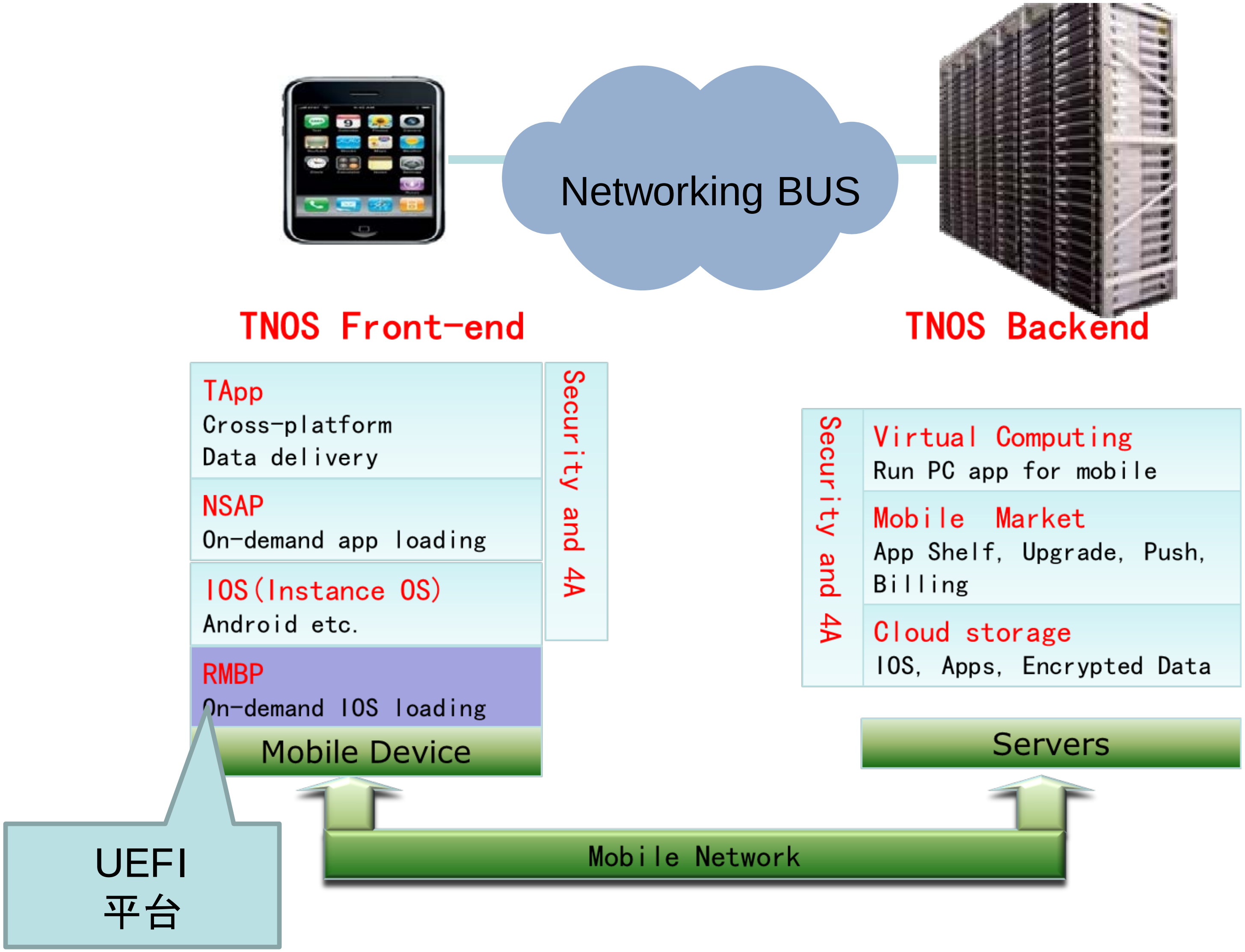
# 当前解决方案

## 当前方案没有很好地解决问题

- 用户端反病毒软件
- 云端杀毒服务
- 云端备份
- 付费修复/备份服务
- 专业咨询

*其他解决方案?*

# 卓望基于透明计算的移动设备解决方案



Networking BUS

TNOS Front-end

TApp
Cross-platform
Data delivery

NSAP
On-demand app loading

IOS(Instance OS)
Android etc.

RMBP
On-demand IOS loading

Mobile Device

Security and 4A

TNOS Backend

Security and 4A

Virtual Computing
Run PC app for mobile

Mobile Market
App Shelf, Upgrade, Push, Billing

Cloud storage
IOS, Apps, Encrypted Data

Servers

Mobile Network

UEFI
平台

# 什么是透明 / 如何透明

| 资产 | 前端 | 后端 |
|---|---|---|
| 操作系统实例 | 分发、加载、运行、缓存、完整性验证 | 存储、管理、维护 |
| 应用软件 | 分发、加载、运行、缓存、完整性验证 | 存储、管理、维护 |
| 用户数据 | 生成、显示、缓存 | 存储、加密 |

# 透明数据存储

即拍即存

## 传统方案

```
Capture();
fwrite(“C:\temp\picture.jpg”);
new soket to server;
Write to socket;
Close soket;
```

## 透明计算

```
Capture();
fwrite(“C:\temp\picture.jpg”);
```

C: is transparently mapped to back-end storage

# 对移动运营商的作用

- 操作系统管理
  - 安全
  - 不受恶意软件的侵害
- 设备缺陷控制
  - 应用软件集中管理
  - 自动升级
  - 拒绝风险软件
- 高性能网络
  - 垃圾流量抑制

# 面临的问题和解决方案

## 无线

低带宽
低可靠性

本地缓存
虚拟磁盘管理

## 可管理性

从面向设备到面向用户

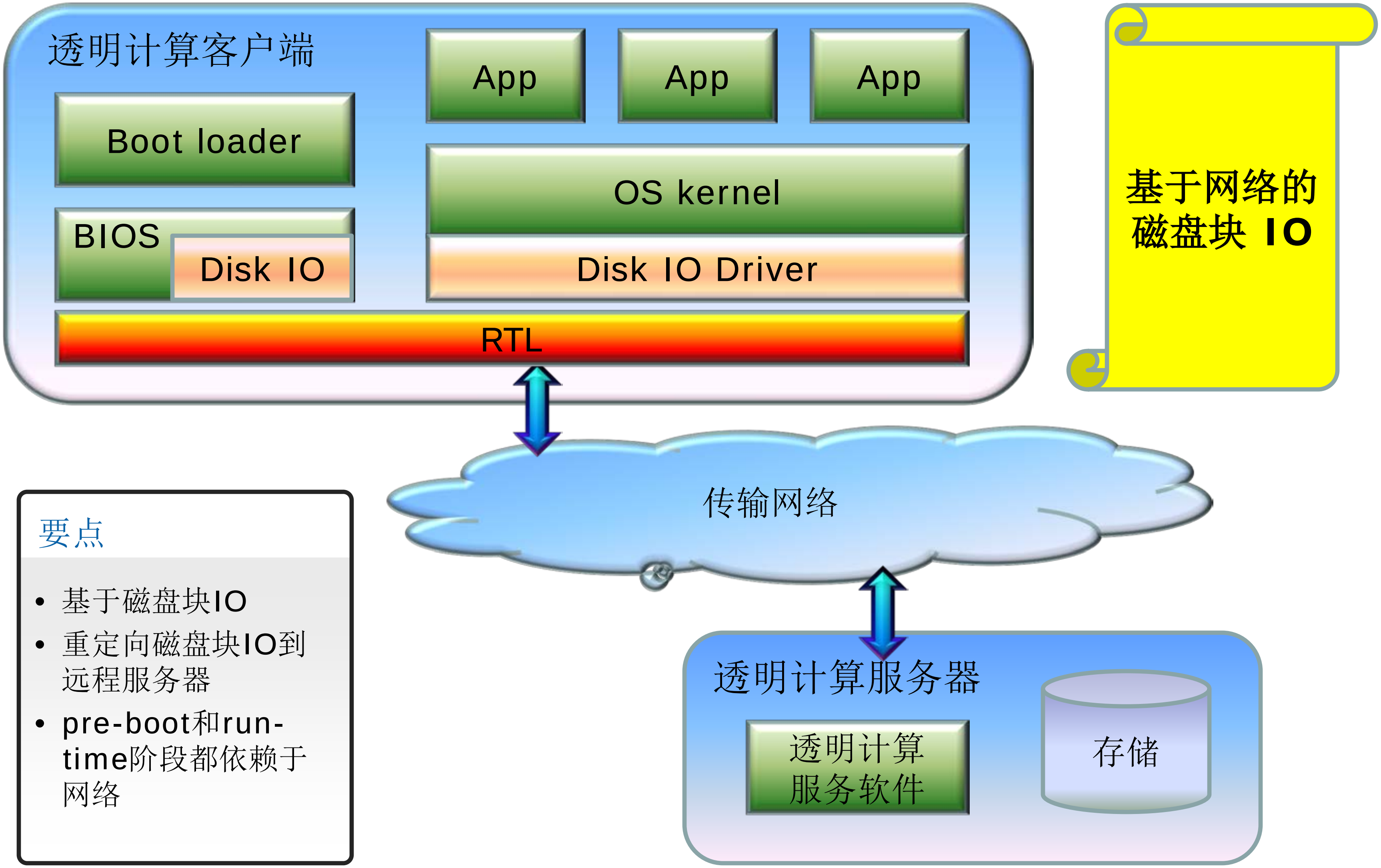
- BIOS层面启动映像管理
- BIOS层面用户管理

## 操作系统无关

多操作系统支持
非开源系统支持

- 基于磁盘块的IO
- 不依赖于特定的文件系统

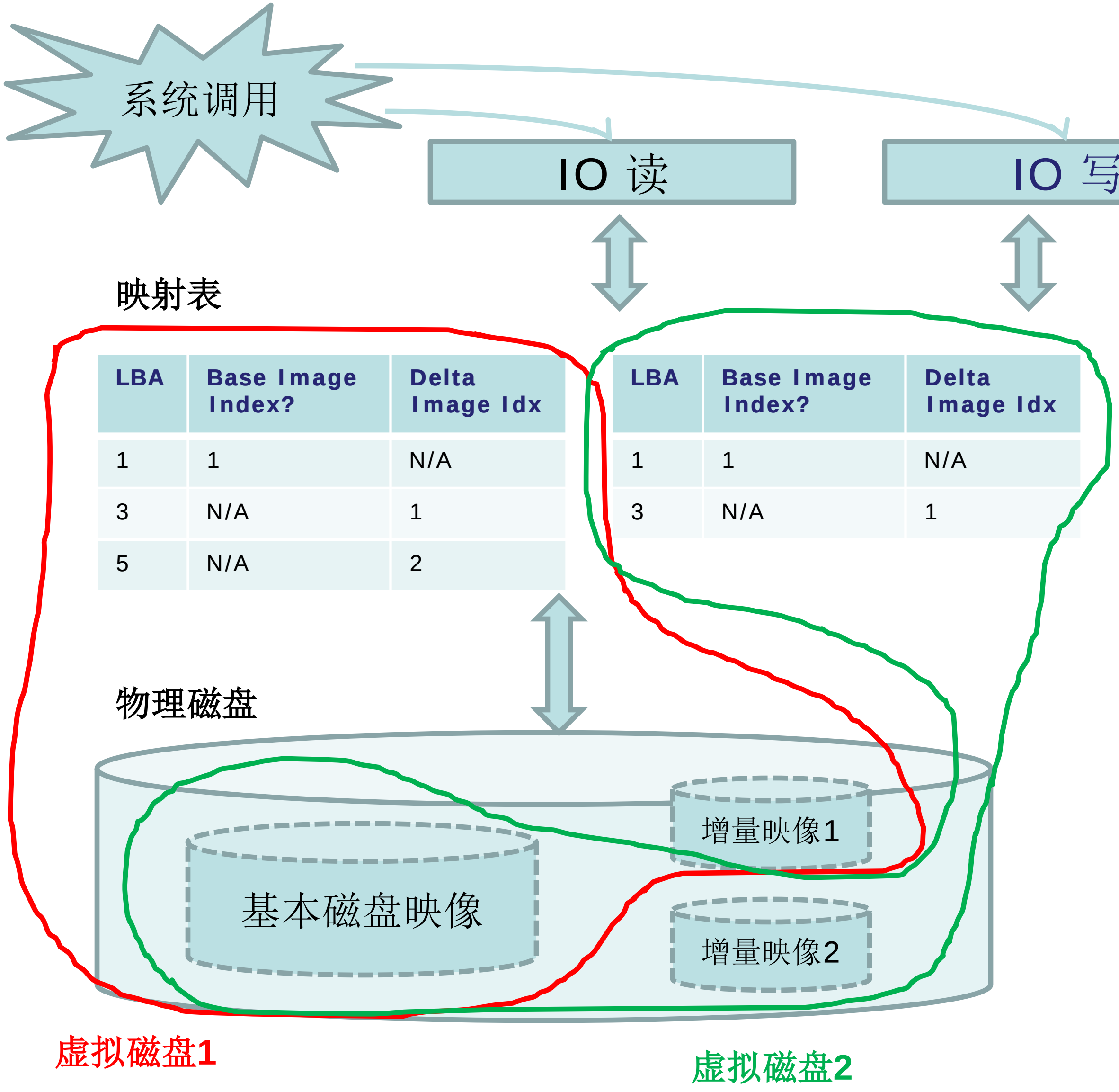
# 非虚拟透明计算方案回顾 – 体系结构



要点

- 基于磁盘块IO
- 重定向磁盘块IO到远程服务器
- pre-boot和run-time阶段都依赖于网络

# 非虚拟透明计算方案回顾 – 虚拟磁盘管理



| LBA | Base Image Index? | Delta Image Idx |
|---|---|---|
| 1 | 1 | N/A |
| 3 | N/A | 1 |
| 5 | N/A | 2 |

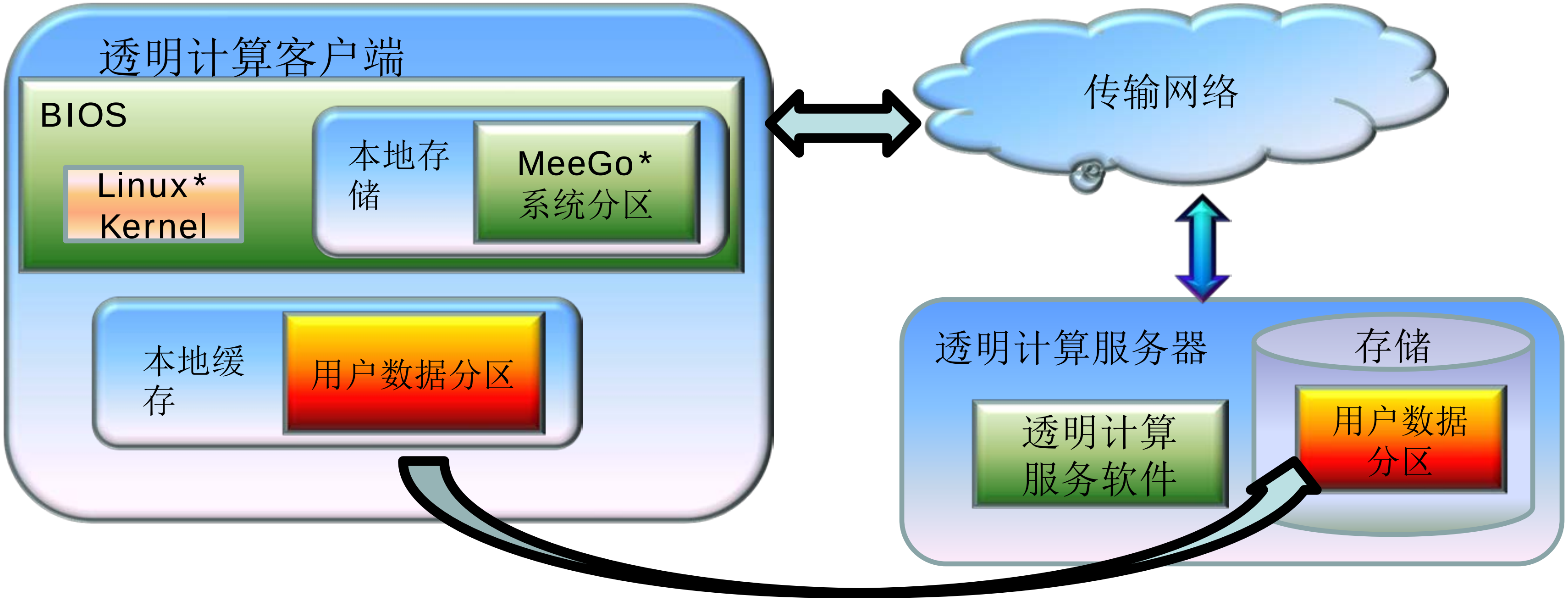
| LBA | Base Image Index? | Delta Image Idx |
|---|---|---|
| 1 | 1 | N/A |
| 3 | N/A | 1 |

**虚拟磁盘管理**

要点

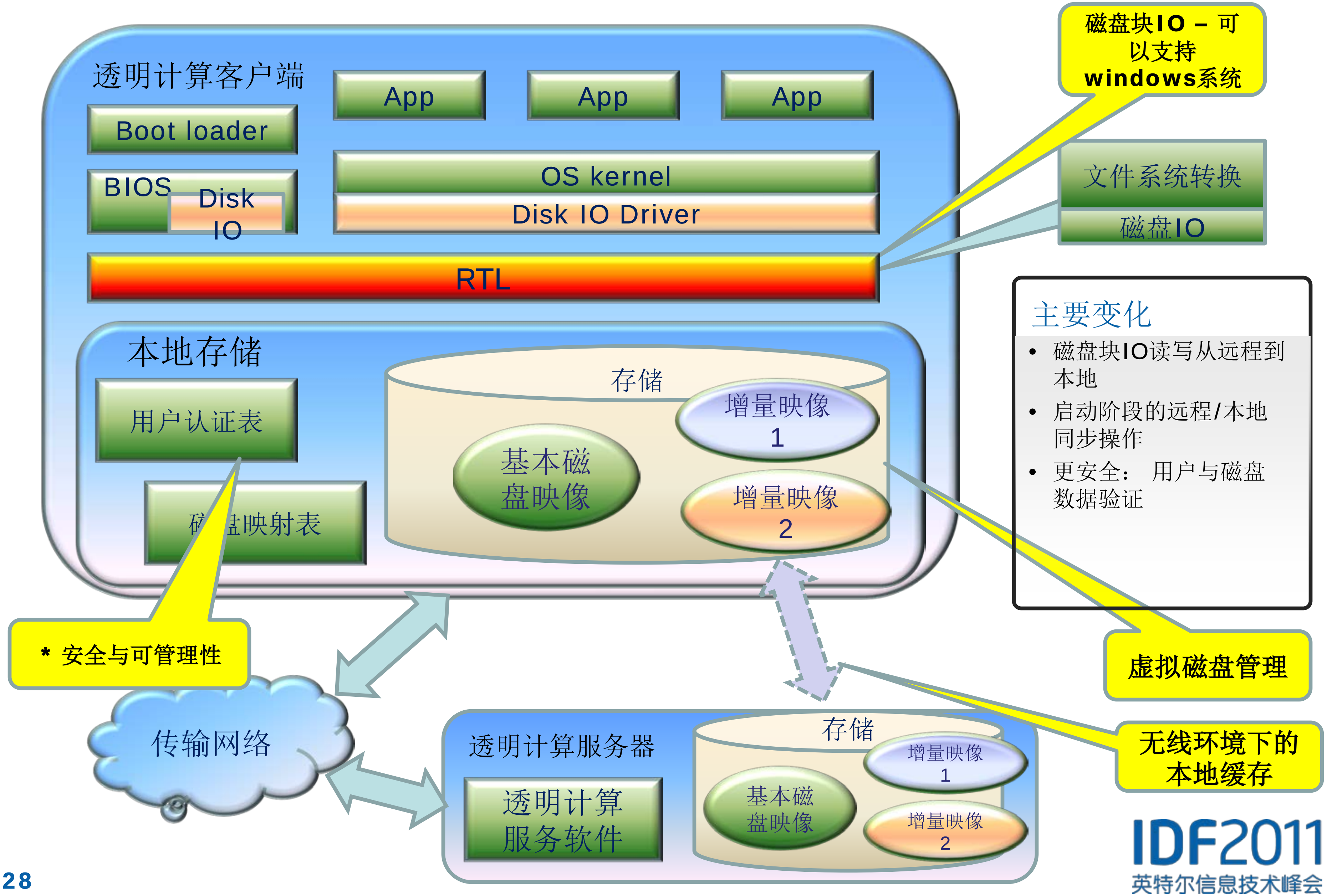
- 虚拟磁盘映像 = 映射表 + 基本映像 + 增量文件
- 不同的虚拟磁盘映像共享相同的基本映像
- 映射表 + 增量：监测磁盘修改记录

# 基于Linux的卓望透明计算解决方案回顾



- BIOS内嵌入定制的Linux系统
- 基于文件系统的缓存更新
- 只更新用户数据分区，系统分区不更新

# 操作系统无关的透明计算解决方案（卓望新方案）



磁盘块IO – 可以支持windows系统

* 安全与可管理性

虚拟磁盘管理

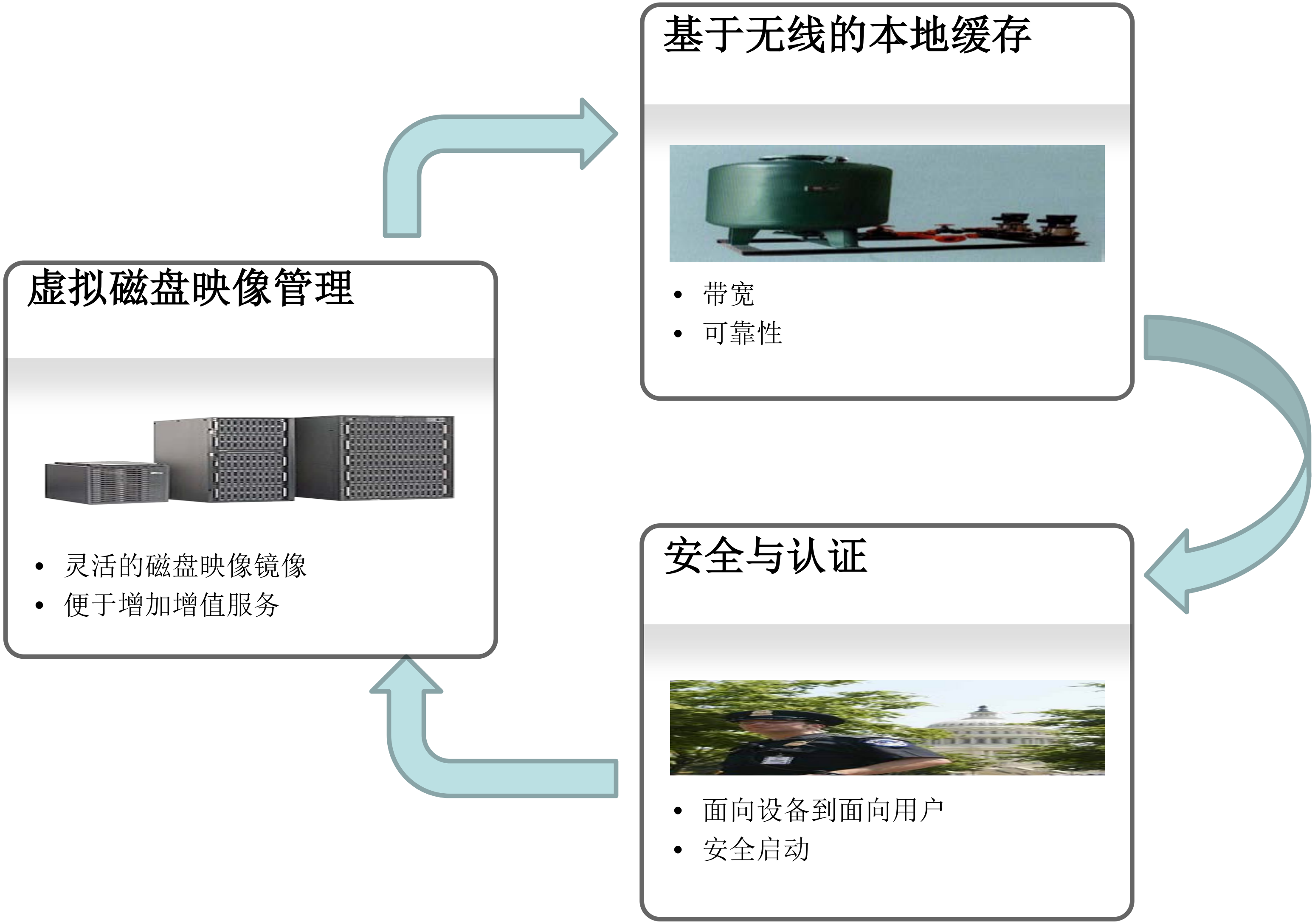
无线环境下的本地缓存

## 主要变化

- 磁盘块IO读写从远程到本地
- 启动阶段的远程/本地同步操作
- 更安全： 用户与磁盘数据验证

IDF2011 英特尔信息技术峰会

# UEFI对卓望方案的贡献



## 基于无线的本地缓存

- 带宽
- 可靠性

## 安全与认证

- 面向设备到面向用户
- 安全启动

## 虚拟磁盘映像管理

- 灵活的磁盘映像镜像
- 便于增加增值服务

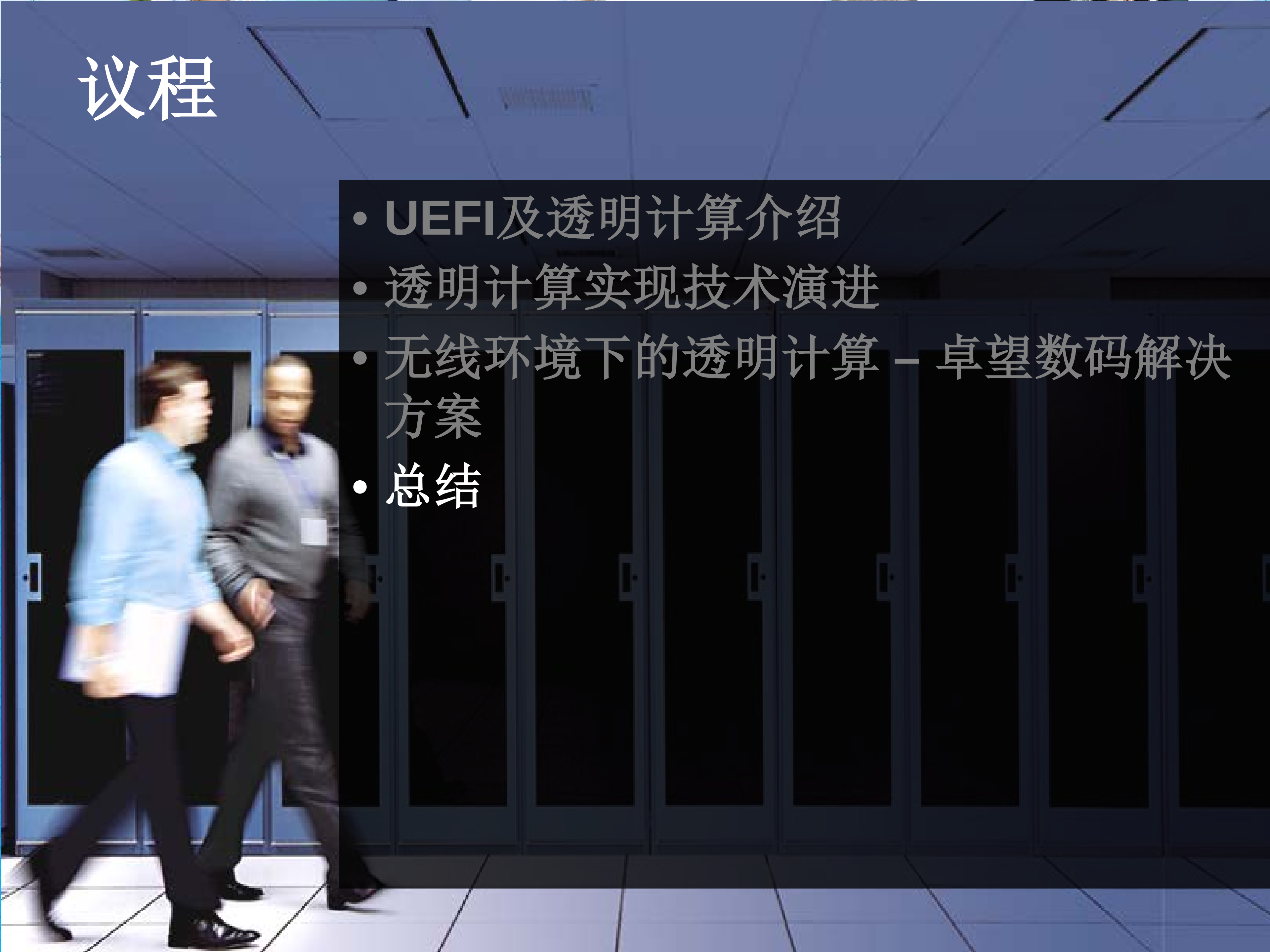
# 演示

- Linux*/MeeGo*透明计算演示
  - 中移动/卓望示范业务
  - 透明计算对MeeGo移动终端的支持

- Windows*透明计算演示
  - BIOS增值服务

# 未来工作规划

- 存储管理
  - 远程/本地磁盘读写智能切换
- 安全
  - 用户认证
  - 磁盘映像安全启动
  - 通过软件服务防止软件盗版
- 可管理性
  - 移动运营商的可管理性
  - 可扩充到行业产品领域



# 议程

- UEFI及透明计算介绍
- 透明计算实现技术演进
- 无线环境下的透明计算 – 卓望数码解决方案
- 总结

# 总结

- 透明计算 – 通过软硬件分离实现“软件即服务”
- 卓望方案 – 基于无线网络、与操作系统无关、面向设备到面向用户的转换
- UEFI和透明计算 – 在BIOS内增加增值服务，更安全更灵活
- 基于UEFI的创新

# Additional resources on UEFI:

- Other UEFI Sessions – Next slide
- More web based info:
  - Specifications sites www.uefi.org, www.intel.com/technology/efi
  - EDK II Open Source Implementation: www.tianocore.org

- Technical book from Intel Press: “Beyond BIOS: Implementing the Unified Extensible Firmware Interface with Intel’s Framework” www.intel.com/intelpress

# EFI 专题讲座课程

| 课程编号 | 课程标题 | 日期/时间 | 教室 |
|---|---|---|---|
| EFIS001 ✓ | 微软* Windows*平台演进与UEFI规范 | 周二 11:10 | 306A |
| EFIS002 ✓ | 片上系统（SoC）的 UEFI 开发与创新特性 | 周二 14:05 | 306A |
| EFIS003 ✓ | UEFI 和透明计算技术 | 周二 15:10 | 306A |
| EFIS004 | 英特尔® UEFI 开发套件 2010 和英特尔® Boot Loader 开发套件： 高级嵌入式开发基础 | 周二 16:10 | 306A |
| SPCQ001 | 热点问题问答:英特尔® Boot Loader 开发套件（英特尔® BLDK） | 周二 17:00 | 306A |
| EFIS005 | 当前 UEFI 和英特尔® UEFI 开发套件 2010（英特尔® UDK2010）在安全性和网络连接方面的进展 | 周三 11:10 | 306A |

✓ =完毕

# 本课程演示文稿 - PDFs

本课程演示文稿（PDF）发布在技术课程目录网站：

**intel.com / go / idfsessionsBJ**

该网址同时打印于会议指南中专题讲座日程页的上方

# 请填写课程评估表

## 请将您填写完的课程评估表交予大会工作人员

非常感谢您的反馈，我们将据此改进未来的英特尔信息技术峰会

# 问答

# 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 PROPETY 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 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.
- Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark* and MobileMark*, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.
- Intel, Sponsors of Tomorrow. and the Intel logo are trademarks of Intel Corporation in the United States and other countries.
- *Other names and brands may be claimed as the property of others.
-

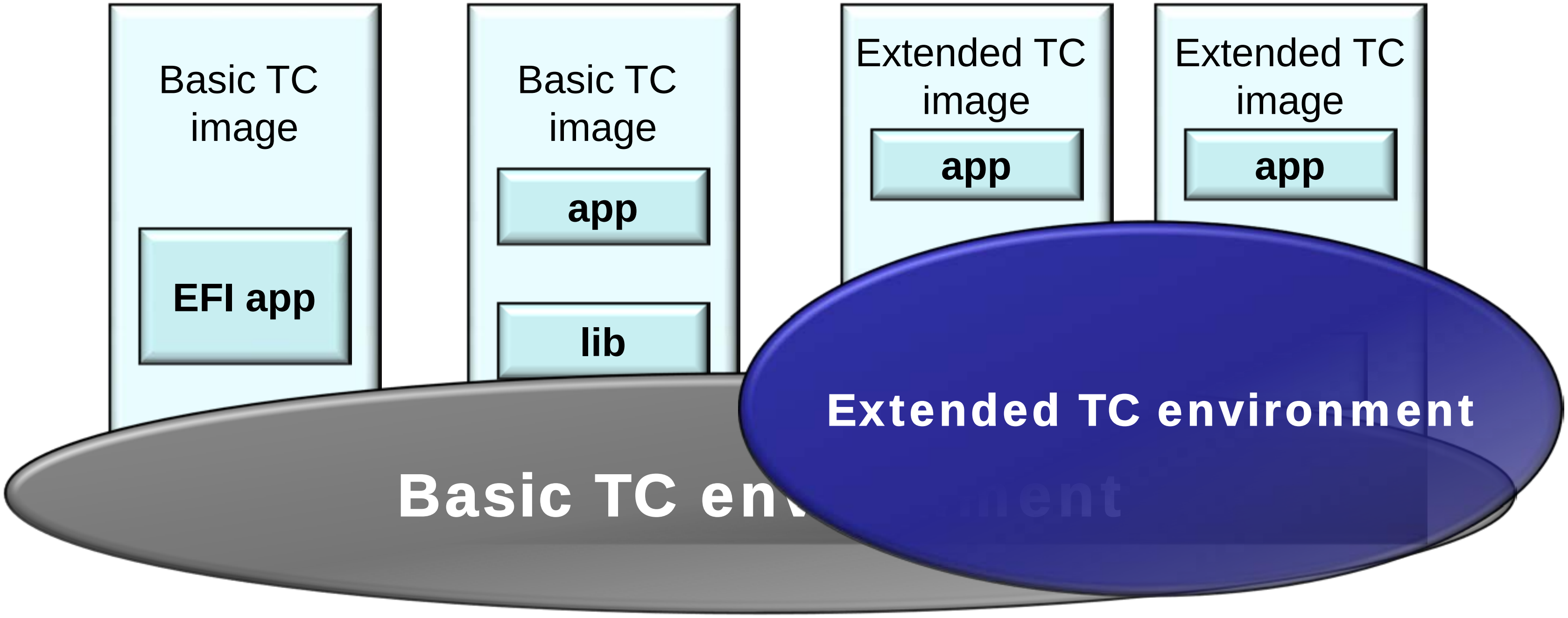
# Risk Factors

The above statements and any others in this document that refer to plans and expectations for the first quarter, the year and the future are forward-looking statements that involve a number of risks and uncertainties. Many factors could affect Intel’s actual results, and variances from Intel’s current expectations regarding such factors could cause actual results to differ materially from those expressed in these forward-looking statements. Intel presently considers the following to be the important factors that could cause actual results to differ materially from the corporation’s expectations. Demand could be different from Intel's expectations due to factors including changes in business and economic conditions; customer acceptance of Intel’s and competitors’ products; changes in customer order patterns including order cancellations; and changes in the level of inventory at customers. Intel operates in intensely competitive industries that are characterized by a high percentage of costs that are fixed or difficult to reduce in the short term and product demand that is highly variable and difficult to forecast. Revenue and the gross margin percentage are affected by the timing of Intel product introductions and the demand for and market acceptance of Intel's products; actions taken by Intel's competitors, including product offerings and introductions, marketing programs and pricing pressures and Intel’s response to such actions; and Intel’s ability to respond quickly to technological developments and to incorporate new features into its products. The gross margin percentage could vary significantly from expectations based on capacity utilization; variations in inventory valuation, including variations related to the timing of qualifying products for sale; changes in revenue levels; product mix and pricing; the timing and execution of the manufacturing ramp and associated costs; start-up costs; excess or obsolete inventory; changes in unit costs; defects or disruptions in the supply of materials or resources; product manufacturing quality/yields; and impairments of long-lived assets, including manufacturing, assembly/test and intangible assets. Expenses, particularly certain marketing and compensation expenses, as well as restructuring and asset impairment charges, vary depending on the level of demand for Intel's products and the level of revenue and profits. The majority of Intel’s non-marketable equity investment portfolio balance is concentrated in companies in the flash memory market segment, and declines in this market segment or changes in management’s plans with respect to Intel’s investments in this market segment could result in significant impairment charges, impacting restructuring charges as well as gains/losses on equity investments and interest and other. Intel's results could be impacted by adverse economic, social, political and physical/infrastructure conditions in countries where Intel, its customers or its suppliers operate, including military conflict and other security risks, natural disasters, infrastructure disruptions, health concerns and fluctuations in currency exchange rates. Intel’s results could be affected by the timing of closing of acquisitions and divestitures. Intel's results could be affected by adverse effects associated with product defects and errata (deviations from published specifications), and by litigation or regulatory matters involving intellectual property, stockholder, consumer, antitrust and other issues, such as the litigation and regulatory matters described in Intel's SEC reports. An unfavorable ruling could include monetary damages or an injunction prohibiting us from manufacturing or selling one or more products, precluding particular business practices, impacting Intel’s ability to design its products, or requiring other remedies such as compulsory licensing of intellectual property. A detailed discussion of these and other factors that could affect Intel’s results is included in Intel’s SEC filings, including the report on Form 10-Q for the quarter ended September 25, 2010.

Rev. 1/13/11

# Backup Slides

# ASPire Solution Based on UEFI



- **Basic TC environment：EFI-based**
  - OS neutral
  - Close to HW, provide HW diagnosis

- **Extended TC environment**
  - Provide public library— public lib is created with Moblin™
  - Provide graphics and network support, easier for app development
  - Can regard extended lib as “part of the BIOS”