构建企业级桌面环境管理系统解决方案

王　　希
IT架构顾问
微软中国有限公司

议　程

- 概述
- 统一桌面管理，核心解决方案与演示
  - 简化部署
  - 软硬件资产管理
  - 保障客户端安全
- 方案设计案例与参考项目流程

IT人士经常碰到的问题

我经常要刻录光盘

我希望能在第一时间打齐所有补丁

我希望能够降低安装驱动程序所带来的风险

我经常碰到问题

要允许我犯错误，但是要有后悔药

我不希望中病毒

安装驱动程序太麻烦了

注册表改坏了

我不希望别人看到我的重要文件

我经常更换电脑

我需要IT专家的帮助

我可能会进行批量部署

我希望实现远程管理

我不希望被攻击

不要试图让我知道哪些文件是重要的

我的系统启动不了了

Windows太庞大了，我不想知道底层的技术

我不想总是跑来跑去

我希望安装操作系统尽量简单和节省时间

我担心由于驱动程序问题导致系统出问题

我怕丢失重要文件

我不希望单独备份

丢失数据是不可接受的

我不希望操作十分复杂

我担心电脑丢失所带来的严重后果

我不想手动打补丁

优化基础架构的关键技术领域

身份及访问管理

桌面系统生命期

安全性、网络和监视

数据保护和恢复

安全、易于管理的邮件系统

基本 | 标准化 | 合理化 | 动态

桌面管理需求

简化部署

- 远程软件自动分发，升级
- 分支机构与移动用户补丁更新支持
- 桌面系统的标准配置

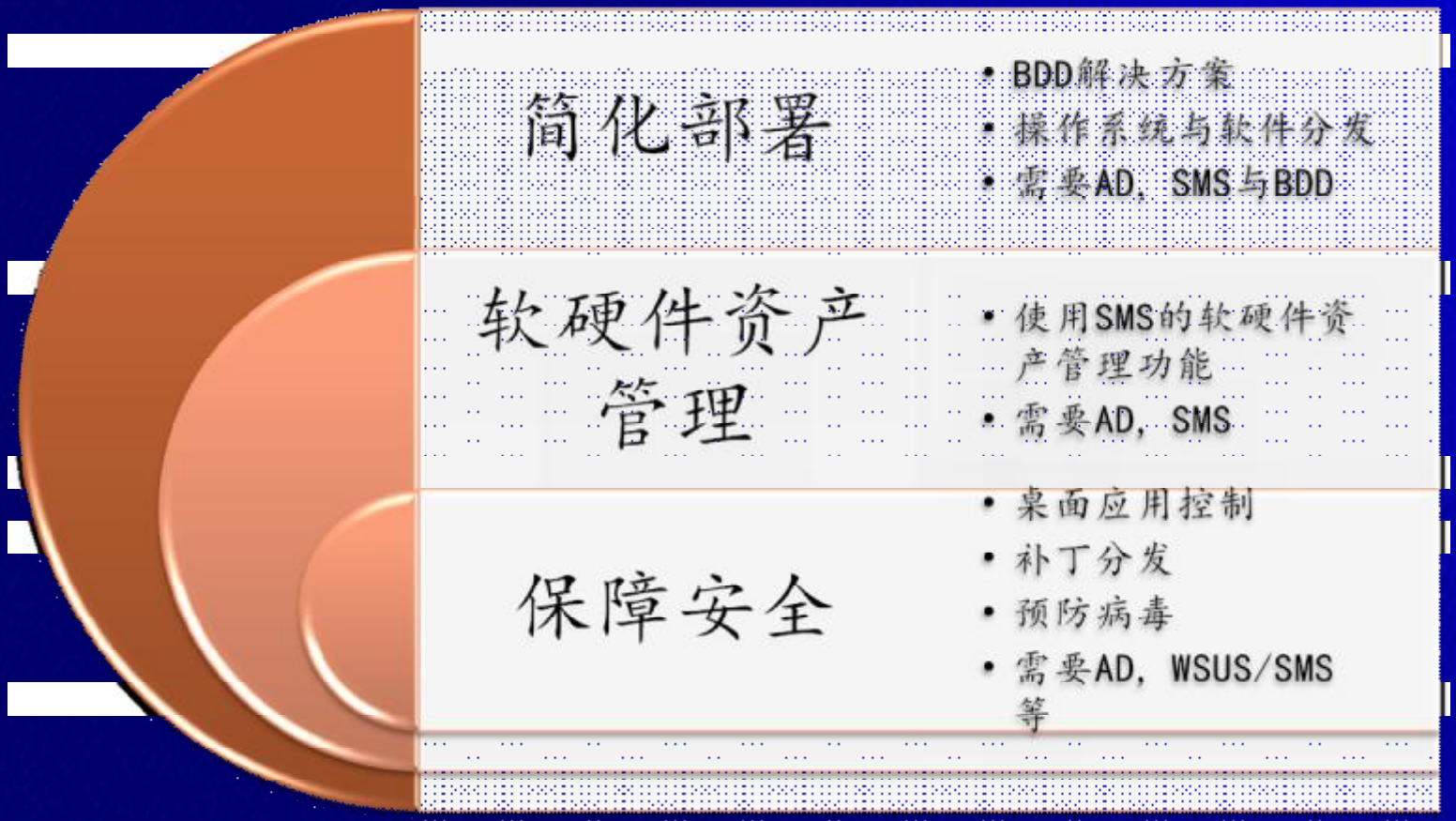
软硬件资产管理

- 硬件资产
- 安装的操作系统
- 安装的应用软件

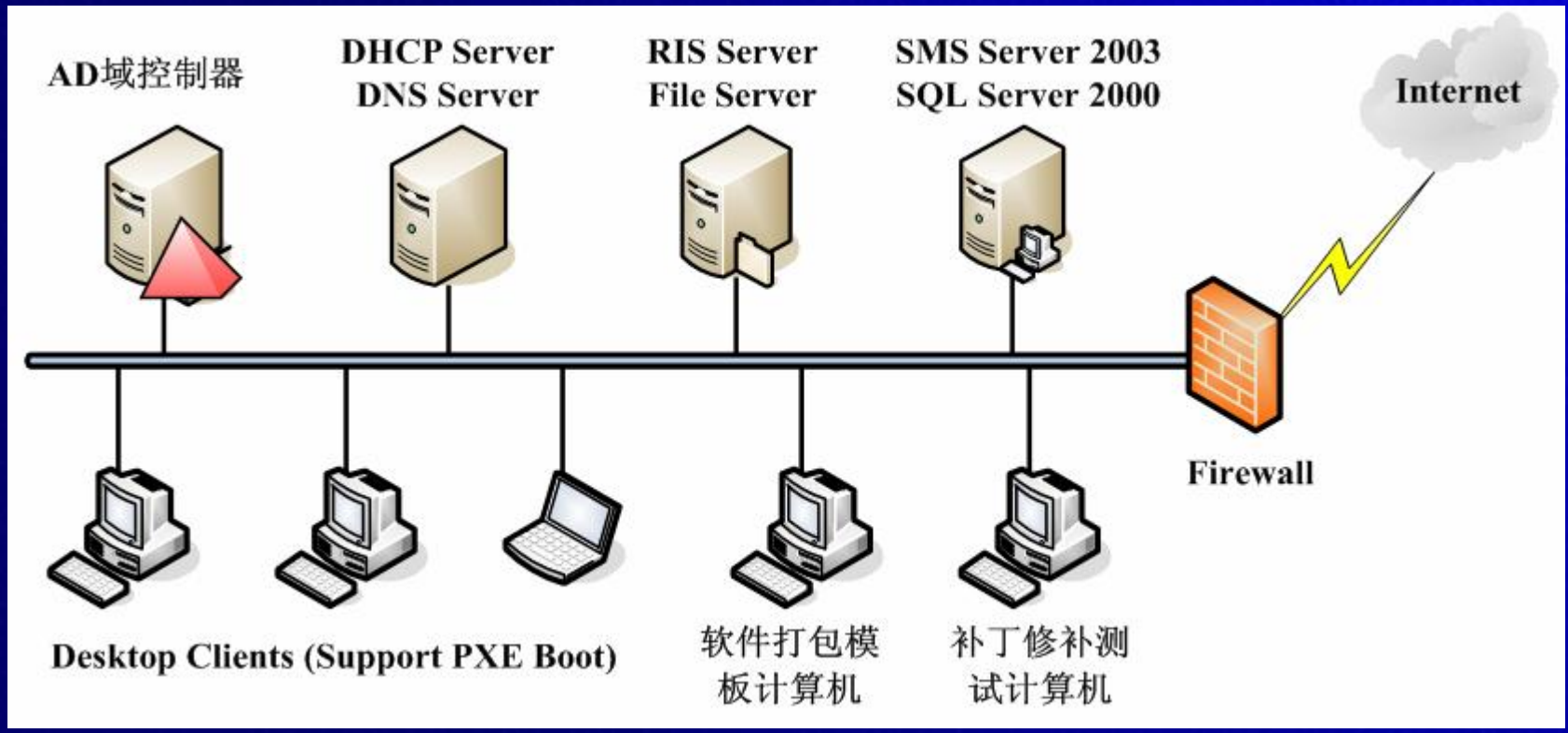
保障安全

- 定位安全弱点，报告缺少的补丁
- 自动下载安装系统补丁，修复系统漏洞
- 实现对桌面应用的控制

桌面管理常见解决方案



统一桌面管理解决方案架构



1. 商业客户端部署
2. 应用软件管理
3. 资产信息收集
4. 用户环境管理
5. 桌面安全管理

议　程

- 概述
- 统一桌面管理，核心解决方案与演示
  - 简化部署
  - 软硬件资产管理
  - 保障客户端安全
- 方案设计案例与参考项目流程

远程系统安装

- 基于网络的远程操作系统安装部署
- 为不同的用户群组、不同的硬件环境准备不同的系统映像
- 并非简单的硬盘克隆，相同的系统映像，不同的系统标识配置
- 自动加入计算机到AD域环境
- 自动产生新的SMS Client ID，接受SMS Server管理
- 系统环境和产品要求：
  - Windows AD域环境
  - DHCP Server、DNS Server
  - SMS Server 2003
  - SQL Server 2000
- 所采用技术：
  - BDD技术
  - Windows 2003 RIS技术
  - Windows AD组策略技术

应用软件管理

- 支持“推”式和“拉”式两种应用软件部署方式
- 结合SMS 2003资产管理技术，实现详细的应用软件部署规划
- 通过软件打包技术，实现应用软件在客户端的无人值守自动部署
- 详细的软件安装状态反馈，了解软件分发的进程和结果报告
- 系统环境和产品要求：
  - Windows AD域环境
  - 文件服务器（Apps Packs）
  - SMS Server 2003
  - SQL Server 2000
- 所采用技术：
  - SMS软件打包技术
  - SMS 2003软件分发技术
  - SMS 2003资产管理技术
  - Windows AD组策略技术

企业桌面终端的部署方式

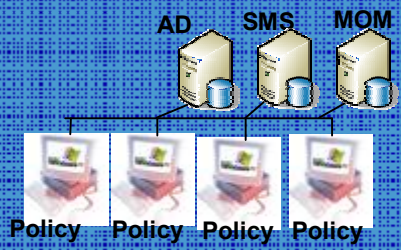
手动的

- 使用CD/DVD等介质存放安装文件
- 从文件服务器安装应用程序
- 有限的用户状态迁移

半自动

- 基于Pull的安装，映像存于网络或者介质
- 系统映像部署后自动安装应用，可能需要使用脚本配置
- 部分实现用户状态迁移或备份与恢复

全自动



- SMS/OSD – to push a WIM based image and patches
- 使用SMS进行自动软件安装
- 用户状态被保留并恢复

微软部署解决方案

商业桌面部署解决方案加速器（BDD）

两个版本 – 一套架构

标准版 vs. 企业版

	标准版	企业版
客户配置文件	拥有250 台或更多 PC 的中等规模客户	拥有 500 台或更多 PC 的企业客户
受支持的情境	▌基于网络的轻量接触部署 ▌被隔离的用户（基于 CDROM/DVD 的安装）	▌支持新计算机、升级计算机和替换计算机方案的零接触安装（基于 SMS） ▌基于网络的轻量接触部 ▌隔离的用户（基于 CDROM/DVD 的安装） ▌零接触的软件和服务供应（ZTP）（基于 BizTalk Server） ▌ZTI 不需要 ZTP，但是 ZTP 需要 ZTI
需要的基础结构	至少具有一个服务器和用于存储工作文件和映像，具有足够磁盘空间的局域网	安装了 Microsoft Active Directory、Remote Installation Services (RIS) 和 SMS 2003（能正常用于软件分发）的 Windows 2000 Server，当使用“零接触”供应时需要 Windows Server 2003

BDD关键技术及版本选择

	Standard	Enterprise	
Products and Tools	**Lite Touch**	**Zero Touch Install**	**Zero Touch Provisioning**
Application Compatibility Toolkit 3.0	~	~	~
Access 2003 Conversion Toolkit	~	~	~
Virtual PC & Virtual Server	~	~	~
Windows Pre-Installation Environment (WinPE 1.5)	~	~	~
User State Migration Tool 2.6	~	~	~
Remote Installation Server (RIS) for Windows Server 2003	~	~	~
Symantec DeployCenter Library Ghost Corp Edition	~	~	~
SMS 2003 SP1 & OS Deployment Feature Pack		~	~
Microsoft Operations Manager 2005		~	~
BizTalk Server 2004 (ZTP)			~
Sharepoint Portal Server 2003			~
Solution Accelerator Components			
Solution Accelerator Guidance	~	~	~
Solution Accelerator Tools & Automation	~	~	~

BDD企业版
主要功能

- 创建模板机器的映像
  - OS, apps, configuration, etc
  - BDD Computer Imaging System
- 通过 OSD Wizard 捕获 WIM 映像
- 创建 OSD 包
- 定制 OSD 包设置
- 通过 SMS 分发 OSD 包
- 利用 ZTI 定制 OSD

SMS 2003 OSD Feature Pack

概述

- 基于磁盘映像部署的微软解决方案
- 是SMS 2003 SP1的免费扩展
- 采用WIM映像格式
- 常见的支持场景
  - 操作系统更新
  - 新旧机器替换
  - 新机器安装
- 支持脚本定制
- 支持多种状态迁移工具
- 可扩展支持复杂的应用场景

演　　示

BDD解决方案演示

SMS 2003 OSD Feature Pack

主要功能

机器映像捕获流程（1）

1. Admin configures Master computer
   - OS + Service Packs
   - Applications (Office, etc)
   - SMS Advanced Client

2. Insert Image Capture CD
   - Capture settings
   - Output options
   - Click “Capture”

Prepare Machine

3. Image Capture Wizard prepares computer
   - Sysprep
   - Advanced Client prep
   - Shutdown

机器映像捕获流程（2）

1. Admin configures Master computer
   - OS + Service Packs
   - Applications (Office, etc)
   - SMS Advanced Client

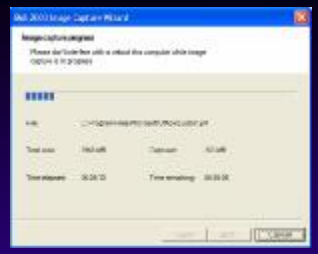
2. Insert Image Capture CD
   - Capture settings
   - Output options
   - Click “Capture”

Prepare Machine

3. Image Capture Wizard prepares computer
   - Sysprep
   - Advanced Client prep
   - Shutdown

Begin Capture

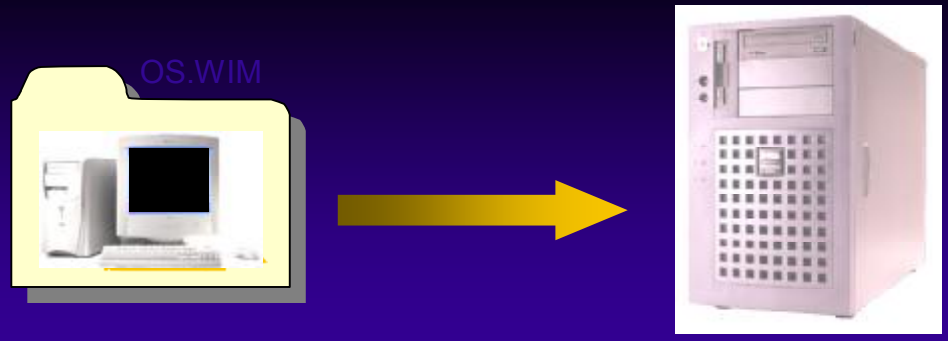
4. Computer boots from Image Capture CD
   - Boot into WinPE
   - Capture wizard continues



5. Capture image
   - Generate WIM image

6. Capture complete

机器映像部署



1. Create image package from captured .wim file

机器映像部署

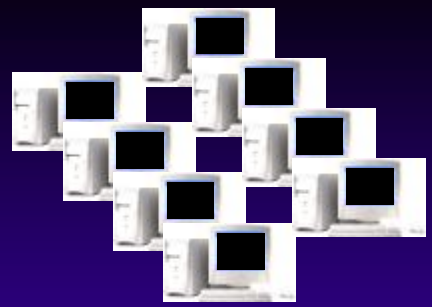
1. Create image package from captured .wim file

2. Configure deployment settings

机器映像部署

1. Create image package from captured .wim file

2. Configure deployment settings

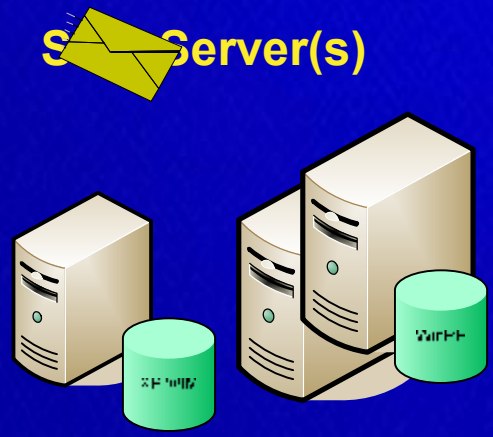


3. Deploy package to distribution points

4. Create collection of target computers to advertise to

OSD 磁盘映像部署
如何实现...

- OSD PE determines SMS DP
- SMS Folder delivers XP WIM package
- OSD modifies sysprep
- Boot partition restored
- System is rebooted
- Mini-setup executes
- Application installs
- USMT restores data
- MiniNT is removed



Existing hard drive partition

SMS 2003 OSD Feature Pack
OSD 内置的定制功能

- Organizational Unit and Domain
- TimeZone
- SMS 2003 Advanced Client
  - SMS GUID
  - SMS Site Membership
- Product ID
- Licensing
- Phase customizations

议　程

- 概述
- 统一桌面管理，核心解决方案与演示
  - 简化部署
  - 软硬件资产管理
  - 保障客户端安全
- 方案设计案例与参考项目流程

资产信息收集

- 强大的设备资产管理功能
  - 发现并跟踪所有Windows计算机信息
- 帮助组织机构制定软件升级计划
- 跟踪计算机与软件资产
- 检查软件许可证的有效性
- 系统环境和产品要求：
  - Windows AD域环境
  - SMS Server 2003
  - SQL Server 2000
- 所采用技术：
  - SMS 2003资产管理技术
  - Windows AD组策略技术

演　　示

软硬件资产管理

议　程

- 概述
- 统一桌面管理，核心解决方案与演示
  - 简化部署
  - 软硬件资产管理
  - 保障客户端安全
- 方案设计案例与参考项目流程

用户环境管理

- 使用户的桌面或系统设置跟着用户移动；不管用户从何处登录到网络，用户都会获得一贯的工作环境，减少熟悉新环境的困惑和时间
- 管理用户设置的能力包括如下的内容：
  - 登录/注销、桌面显示、开始菜单
  - 网络环境、计算机功能限制
  - 本地安全帐号管理、USB存储设备连接限制
  - 本地事件日志管理、注册表修改管理等
- 系统环境和产品要求：
  - Windows AD域环境
  - 文件服务器（User Profiles）
- 所采用技术：
  - Windows AD组策略技术
  - 漫游用户配置文件

桌面安全管理

- 使管理员能够控制修补程序管理
  - 在安装前对更新进行试用和测试
  - 精确控制修补程序管理选项
- 自动完成修补程序管理过程的主要方面
- 可以更新各种各样的 Microsoft 产品
- 通过使用脚本从而具有高度的灵活性
- 系统环境和产品要求：
  - Windows AD域环境
  - 文件服务器（Patches）
  - SMS Server 2003
  - SQL Server 2000
- 所采用技术：
  - ITMU补丁分发技术
  - SMS 2003资产管理技术
  - Windows AD组策略技术
  - Windows Script Host

演　　示

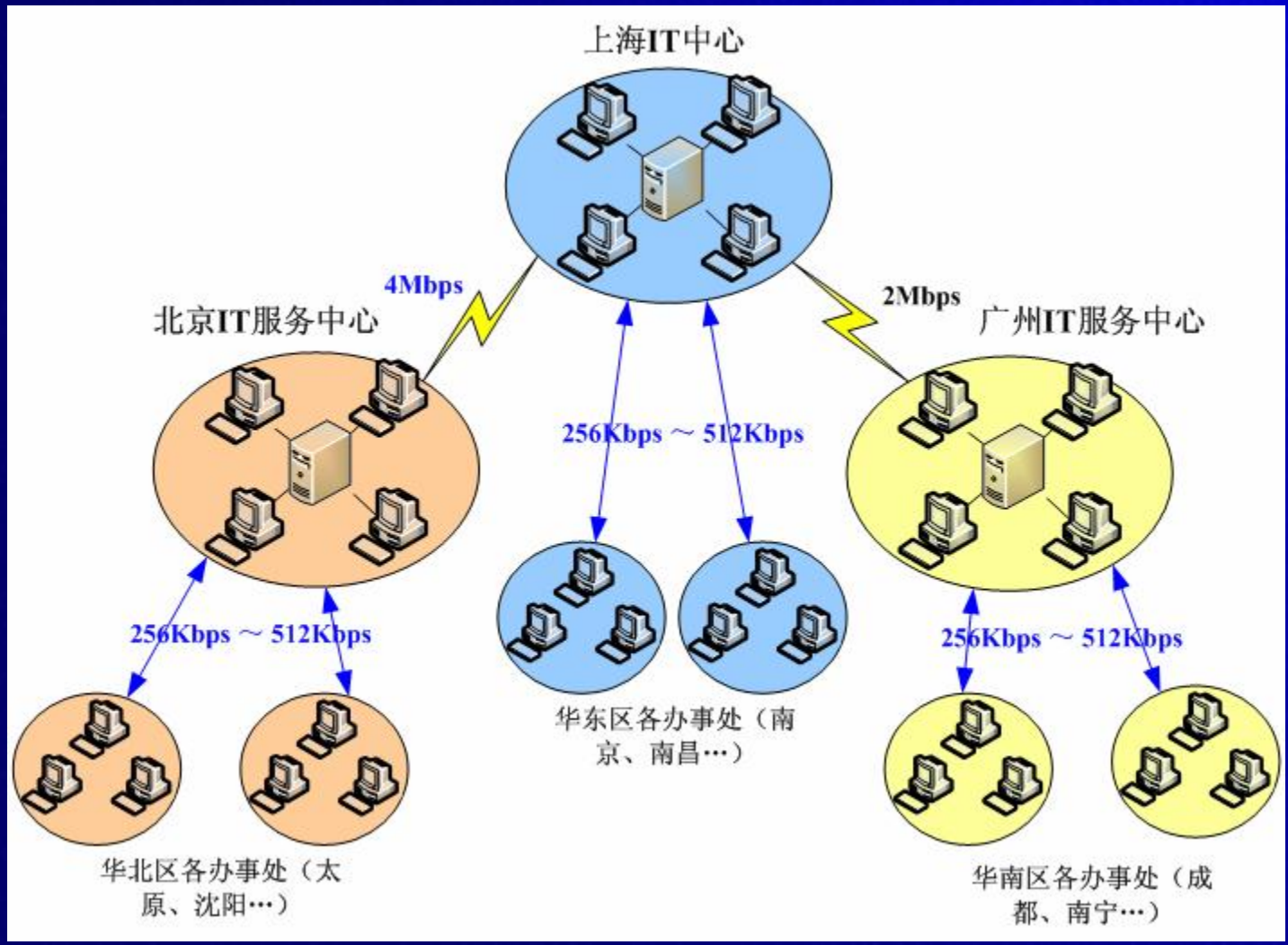
保障客户端安全

- 防止病毒感染
- 桌面应用控制
- WSUS补定管理

议　程

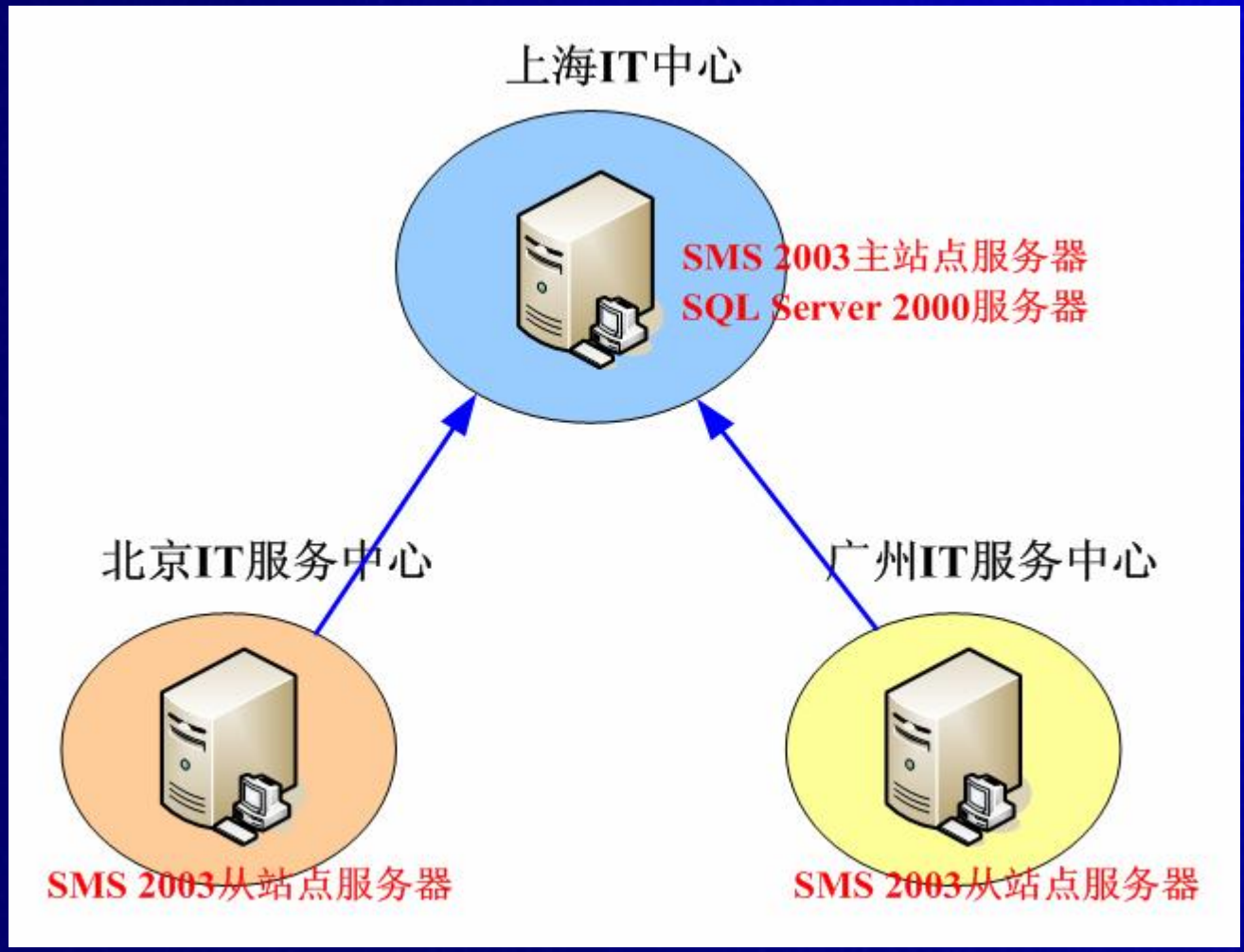
- 概述
- 统一桌面管理，核心解决方案与演示
  - 简化部署
  - 软硬件资产管理
  - 保障客户端安全
- 方案设计案例与参考项目流程

SMS 站点规划

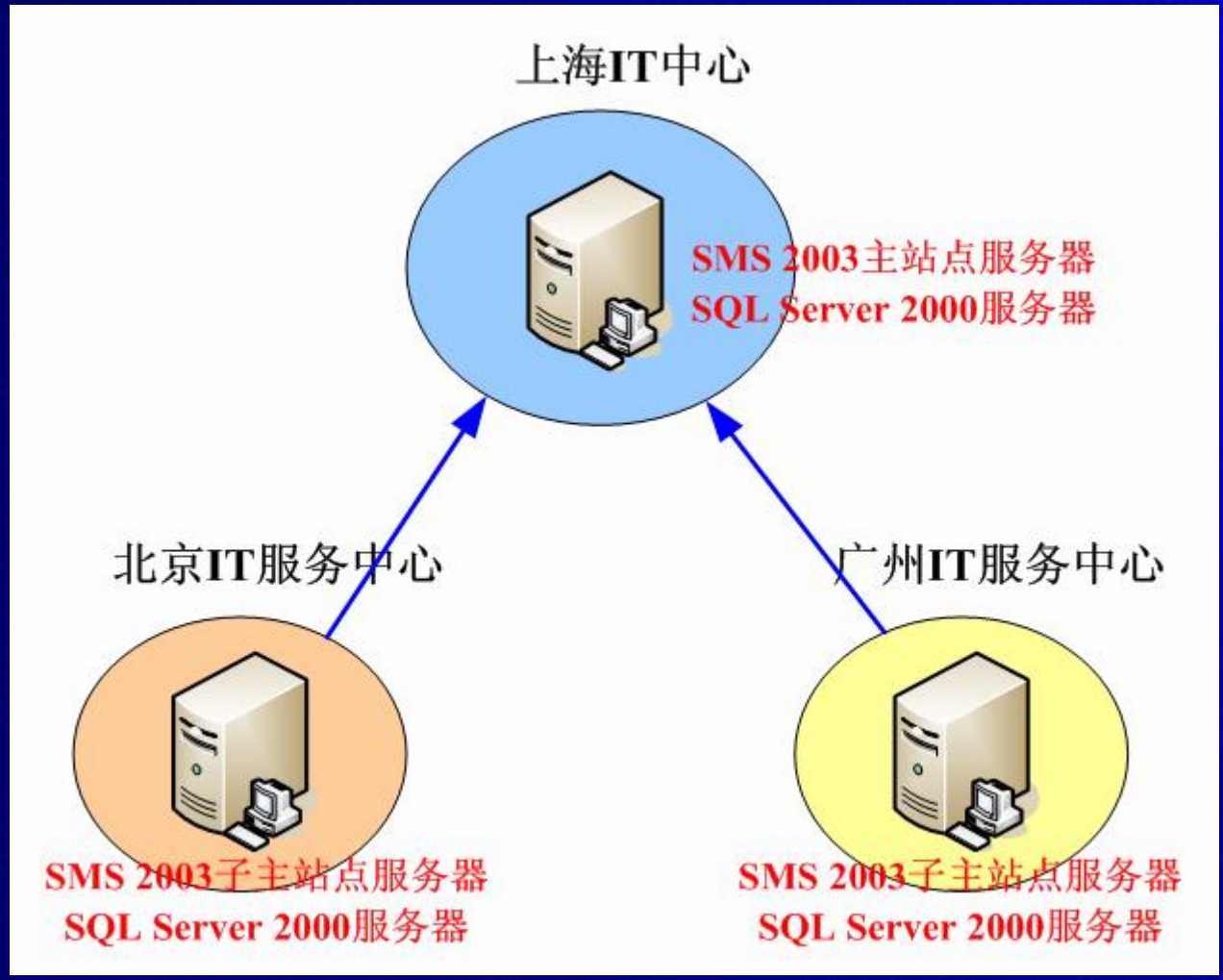


Corp公司网络架构简图

方案A：子从站点架构



方案B：子主站点架构



方案的特性比较

比较项	方案A：子从站点架构	方案B：子主站点架构
本地的IT管理控制能力	• 只能由上海IT中心集中进行统一管理，包括软件分发、补丁管理、资产管理等；	• 可允许上海/广州/北京IT服务中心本地的系统管理人员定制本地的管理策略，如软件分发、资产信息收集等；
本地的报表能力	• 只能在上海IT中心产生整个企业统一的软硬件信息，补丁状态，软件分发状态等报表；	• 可在上海IT中心产生整个企业的报表； • 可允许在广州/北京二级IT服务中心产生本地的信息报表。
软件License采购	• 1个SMS 2003 Server/SQL Tech许可； • 800个SMS Client许可。	• 3个SMS 2003 Server/SQL Tech许可； • 800个SMS Client许可。

系统管理项目实施流程与时间计划

日期	工作任务
项目的准备阶段	
1天	与Corp公司协商实施计划和日程安排
3天	开展项目相关的环境信息的调查，进行部署规划
5天	规划SMS 2003系统
项目的实施阶段	
1天	第一阶段部署SMS中央主站点
2天	第二阶段部署SMS二级站点
3天	第三阶段小规模客户端部署
5天	第四阶段小规模SMS功能测试
15天	第五阶段大规模客户端部署
5天	第六阶段 SMS系统功能实现
系统试运行与调整阶段	
30天	第七阶段 系统的试运行与调整
3天	第八阶段 系统管理员的技能培训
项目的售后服务阶段	
1年	第九阶段 系统售后维护

相关资源

- Microsoft Solution Accelerator for Business Desktop Deployment
  http://www.microsoft.com/technet/desktopdeployment/bddoverview.mspx
- Microsoft Deployment Center
  http://www.microsoft.com/technet/desktopdeployment/default.mspx
- SMS Technical Center
  http://www.microsoft.com/technet/prodtechnol/sms/default.mspx
- 商业客户端部署解决方案系列Webcast
  http://www.microsoft.com/china/technet/webcasts/class/bdd.mspx

TechNet是什么？

- 只需轻轻点击，答案就在您的指尖
  - 对于IT 专业人员来说，TechNet 是一个知识的宝库，你可以找到关于如何规划，部署和管理微软产品的的技术资源

订阅TechNet	u 每月发放包含最新信息的 DVD或者CD Ø 这是最权威的资源，可以帮助你评估、配置和维护微软产品。
TechNet 网站	u 可以访问该站点 www.microsoft.com/china/technet Ø 在线资源和社区 Ø 订户--仅仅提供在线服务
TechNet 中文电子快报	u 两周发放一次的中文电子快报 Ø 安全更新, 新的资源等等
TechNet 活动和网站消息	u 有关最新微软产品介绍和技术的简报 u 上机试验, “如何操作”等信息
中文社区	u 用户群 u 可管理的新闻组

Microsoft TechNet

http://www.microsoft.com/china/technet

我们从哪里可以了解到 TechNet?

- 访问TechNet的官方网站
  www.microsoft.com/China/technet
- 注册TechNet快报
  www.microsoft.com/china/technet/abouttn/subscriptions/flash.mspx
- 加入到中文在线论坛
  http://www.microsoft.com/china/community/
- 成为 TechNet的订户
- www.microsoft.com/china/technet
- 参与到更多的TechNet活动中或者在线了解
  www.microsoft.com/china/technet

您的潜力，我们的动力！

Microsoft

Microsoft TechNet

http://www.microsoft.com/china/technet