



全球运维大会

2016

DevOps 2.0: 重塑运维价值



北京站

会议时间：12月16日 - 12月17日

会议地点：北京国际会议中心

主办单位：



大中型互联网企业IT基础架构概览

陈贻泰 HIM



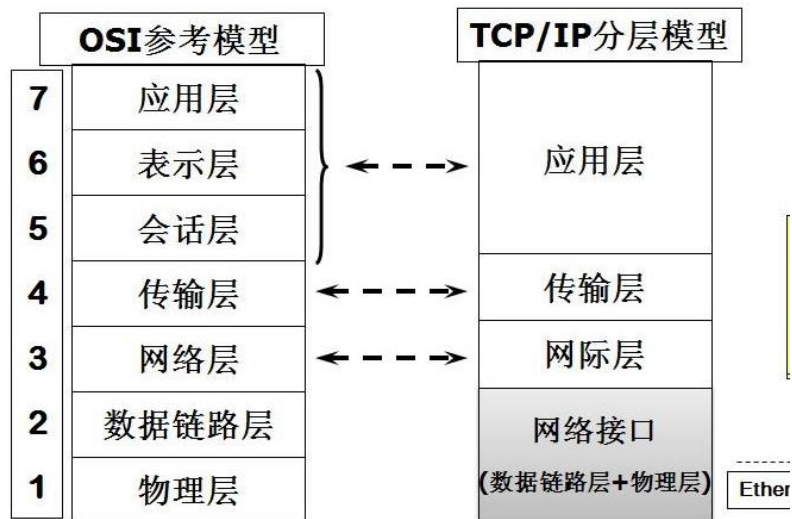
主题介绍

◆自顶向下谈IT基础设施架构

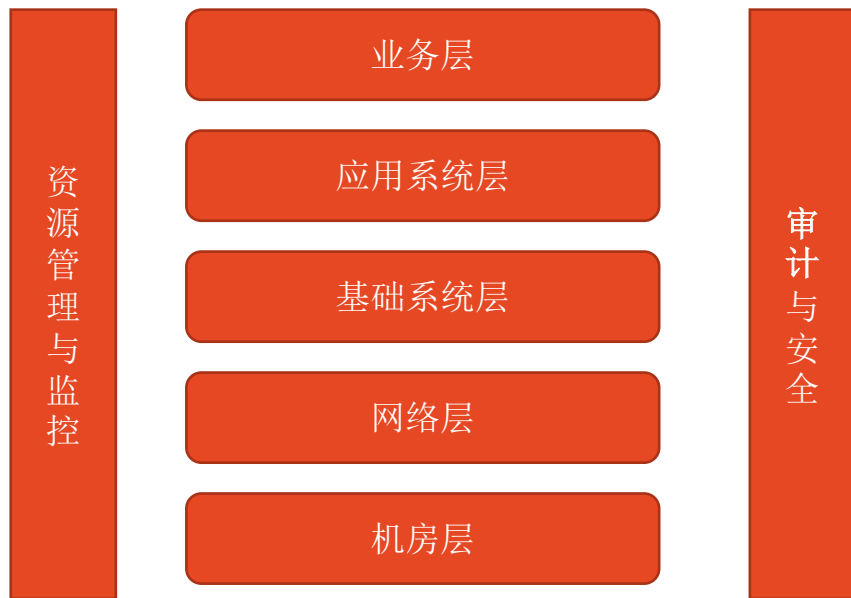
◆IT运维管理之贯彻“五化”



TCP/IP模型给的启示



IT设计模型与实现



- 自顶向下
- 模块化



业务层和应用系统层



企业办公



仓储中心



呼叫中心



快递物流



vancl网



vjia网

- 时间：2011~2013
- 人员：300~13000
- 站点：4~40



GOPS2016
Beijing

基础系统层

- 网络基础服务：DNS、DHCP
- 基础办公：文件、打印
- 企业沟通：邮件、即时通讯、电话
- 信息安全：账户管理、权限
- IT运维：桌面管理、虚拟机管理等



基础系统层之DNS和DHCP

- 高可用
- 易管理



基础系统层之文件打印

- 访问路径统一
- \\vancloa.cn\file\\<departmanetname>
- 空间配额
- 热备和可回滚
- 基于角色的权限设计
- 集中打印系统

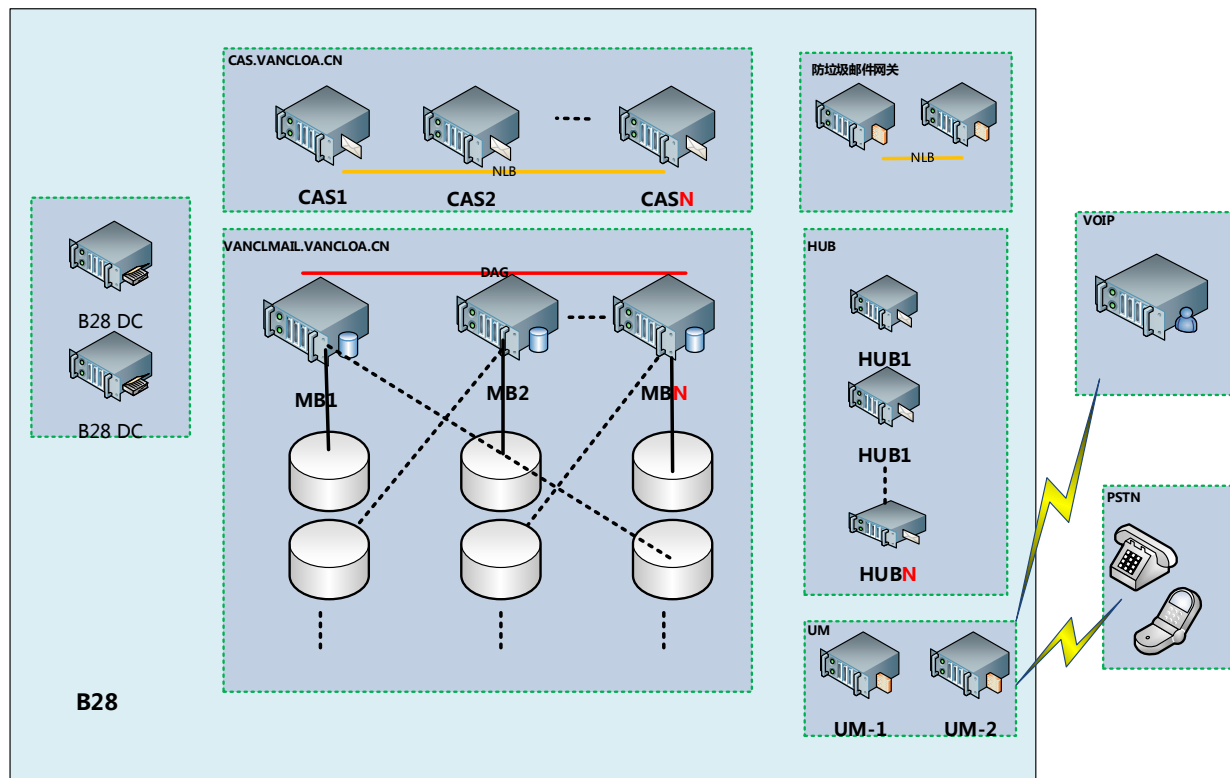


基础系统层之邮件

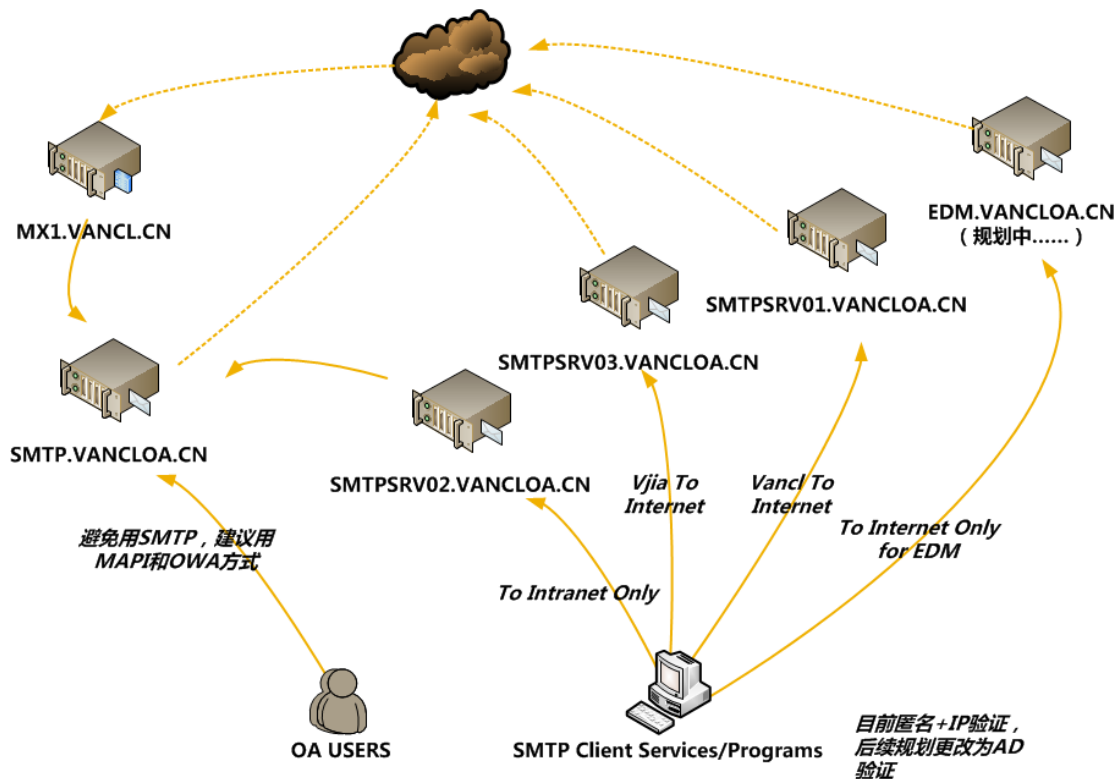
- Exchange
 - （ 邮件收取、办公协作 ）
- Postfix
 - （ 邮件投递、+SpamAssassin防垃圾 ）



基础系统层之Exchange架构



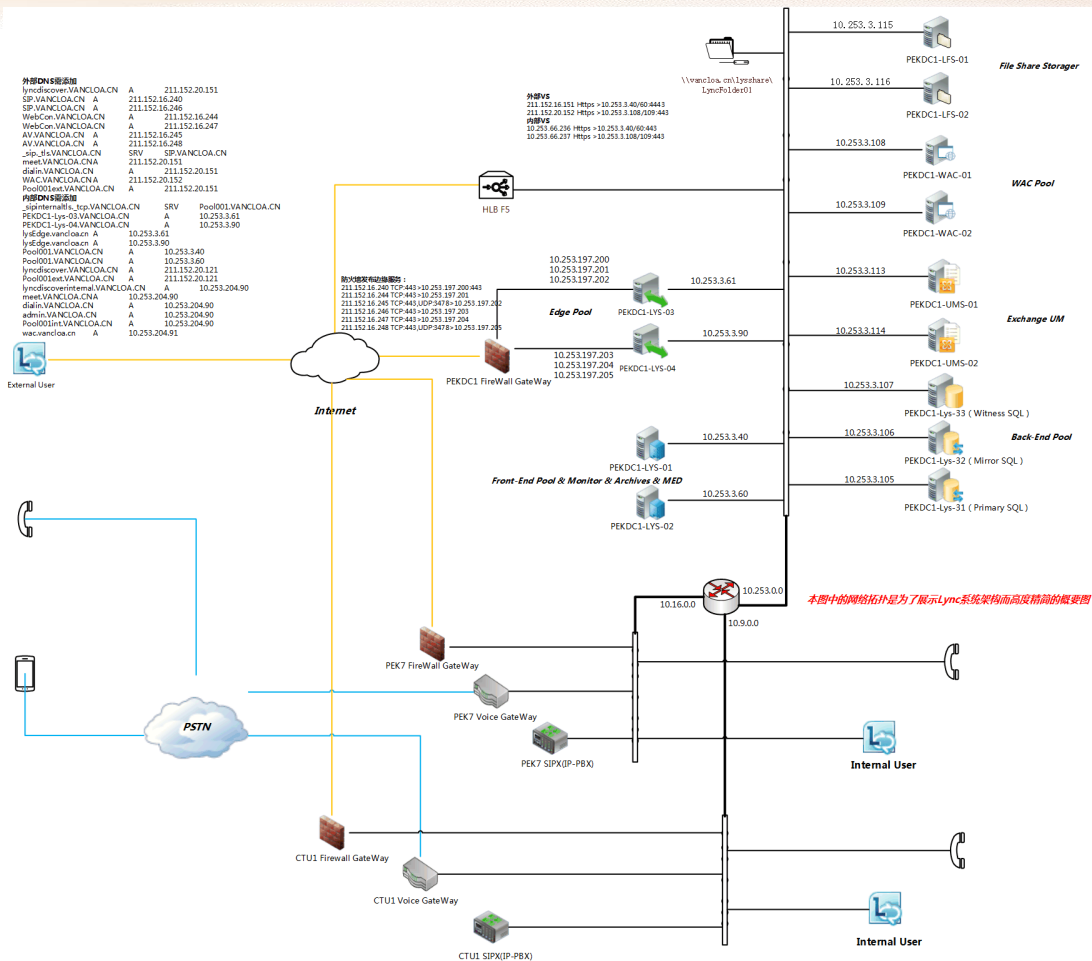
基础系统层之邮件发送流



基础系统之即时通讯

- 电话、语音、视频、邮件、会议
- 手机、话机、PC
- Lync、SIPX、CISCO语音网关、Exchange
- 企业统一沟通，开源与商业软件的结合

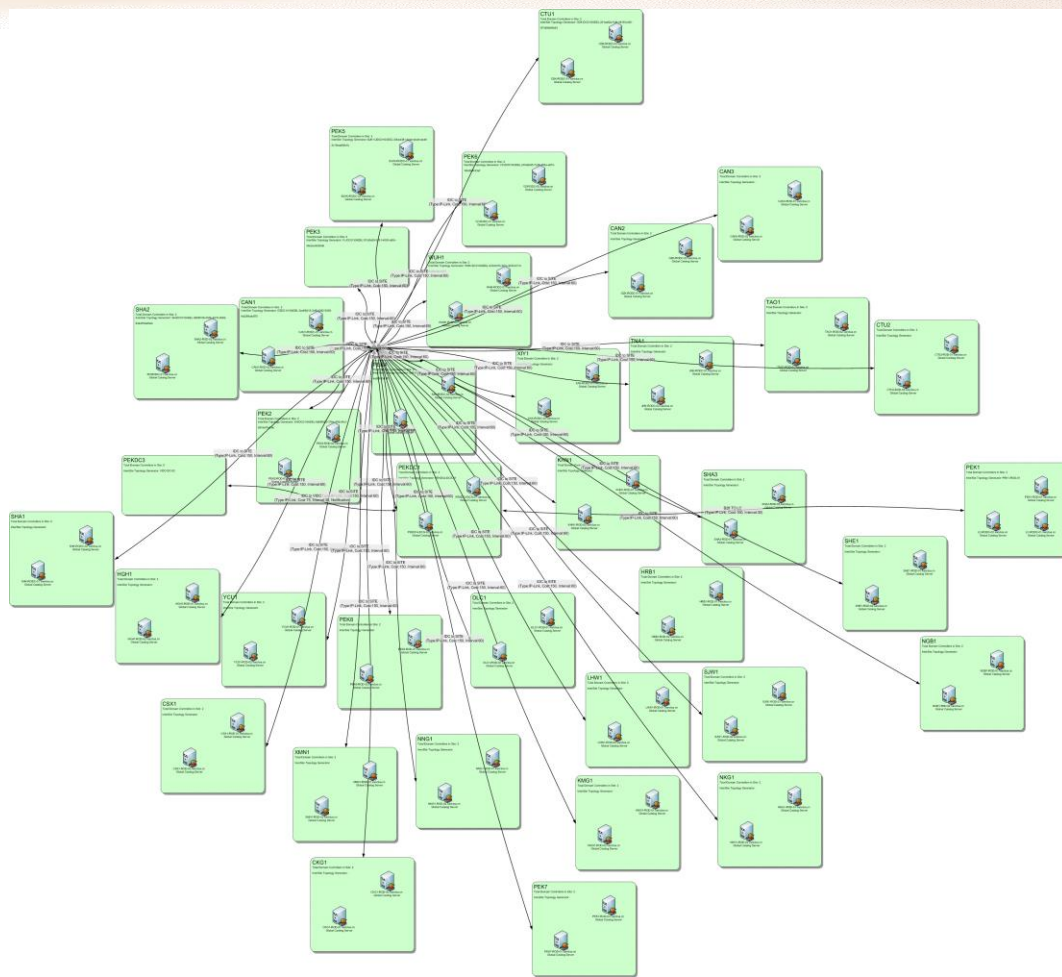




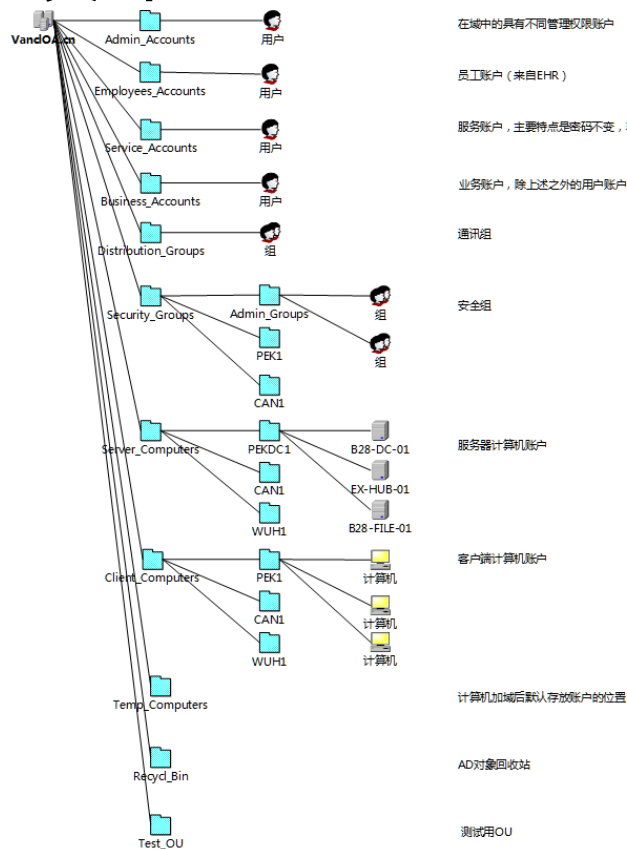
基础系统层之账户与权限

- 活动目录（扁平化和RODC）
- 账户管理自动化、自助化
- 权限管理的两种方式
- 办公与IDC（单向信任，统一管理）
- OA与IT账户（员工信息的自动化管理）
- 网络与系统 ACS（统一管理和权限）





基础系统层之AD设计



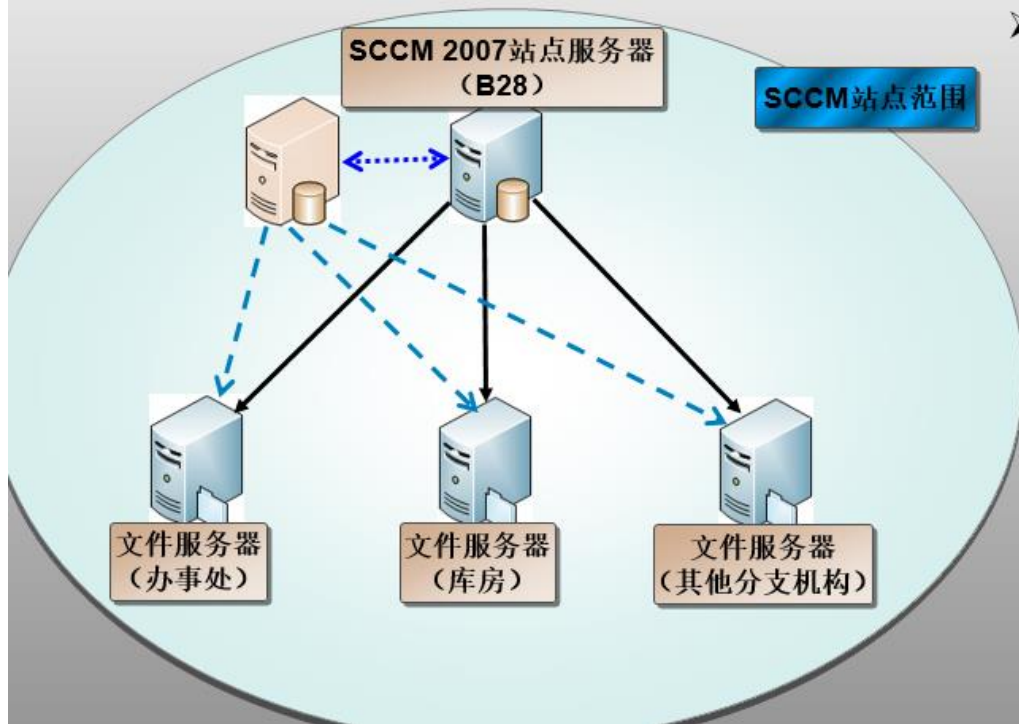
基础系统层之IT运维自动化系统

- 装机、软件分发、远程协助
- 防病毒与系统补丁
- 扁平的CCM架构



基础系统层之IT运维自动化

SCCM 2007 拓扑结构



➤ 使用单站点结构不进行分层设计

➤ 仅B28中心机房部署
SCCM 2007服务器

➤ 各地的分支机构如办事处、库房、呼叫中心等都不需建立**SCCM 2007**专有服务器，仅需在当地文件服务器硬盘上，划分一定空间作为**SCCM**的分发点

➤ 当**SCCM 2007**服务器压力过大时可以增加一台或多台服务器进行负载均衡



基础系统层之虚拟化

- Hyper-v 和KVM
- Openstack + Ceph
- 分布式计算、分布式SDN网络和分布式存储



基础系统层总结

- 企业IT和互联网技术上的不同
- 微软为主，开源为辅，现在又多了一个云产品
- 高可用
- 虚拟化
- 统一的企业账号系统
- 简单大胆的设计

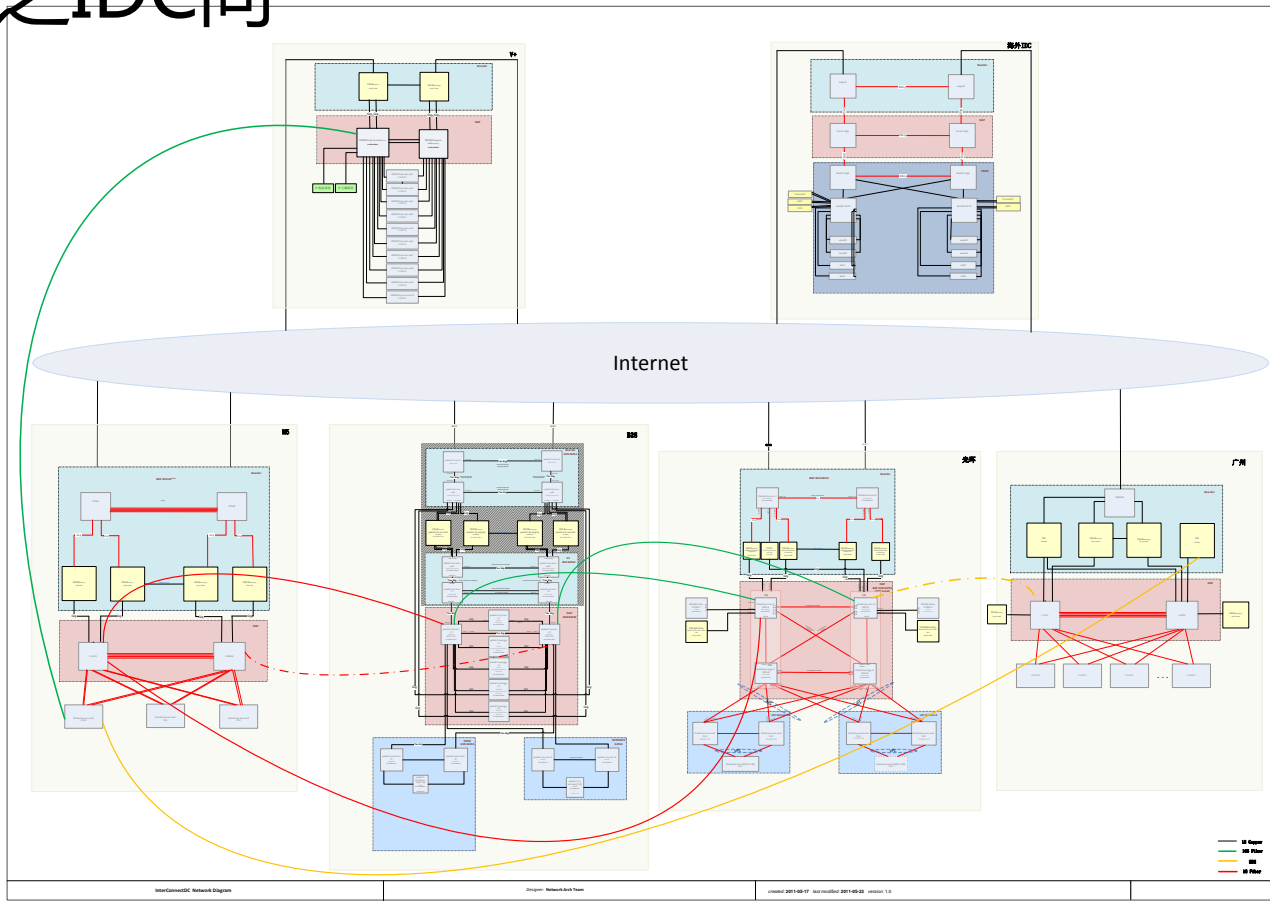


网络层

- IDC间环路
- OSPF + BGP
- ACS与权限管理

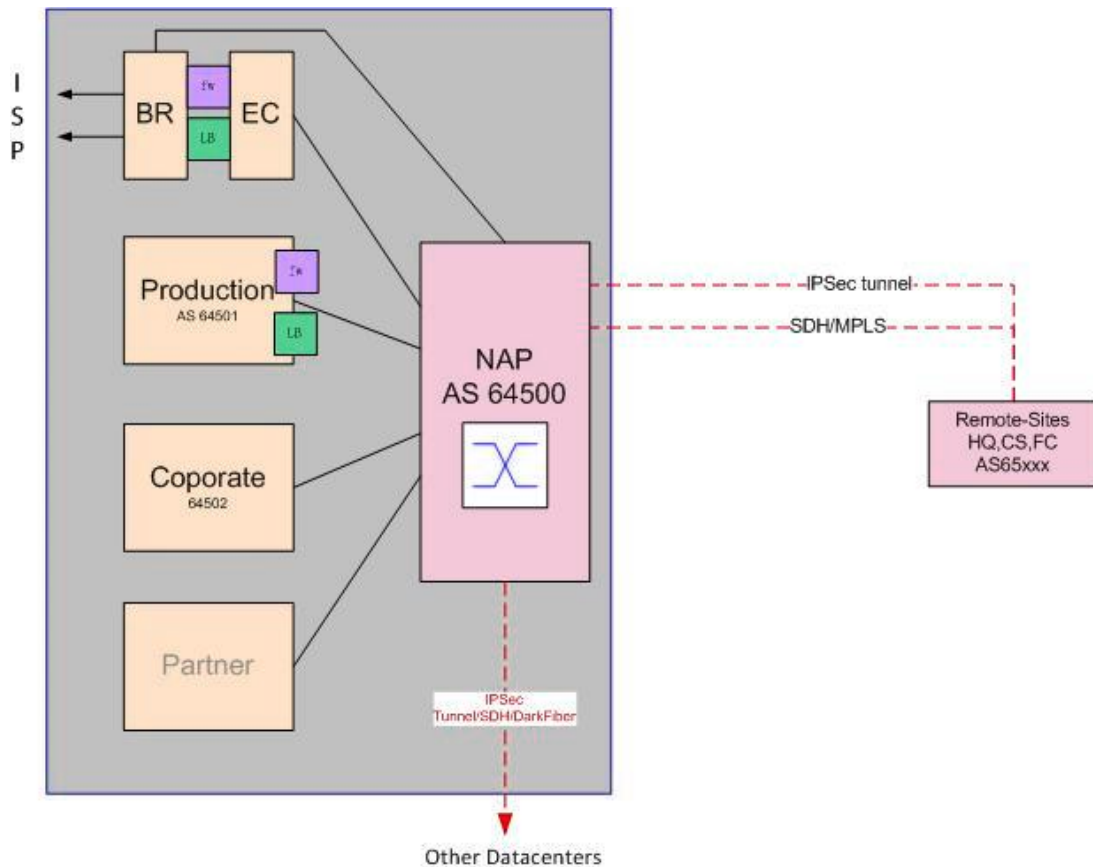


网络层之IDC间



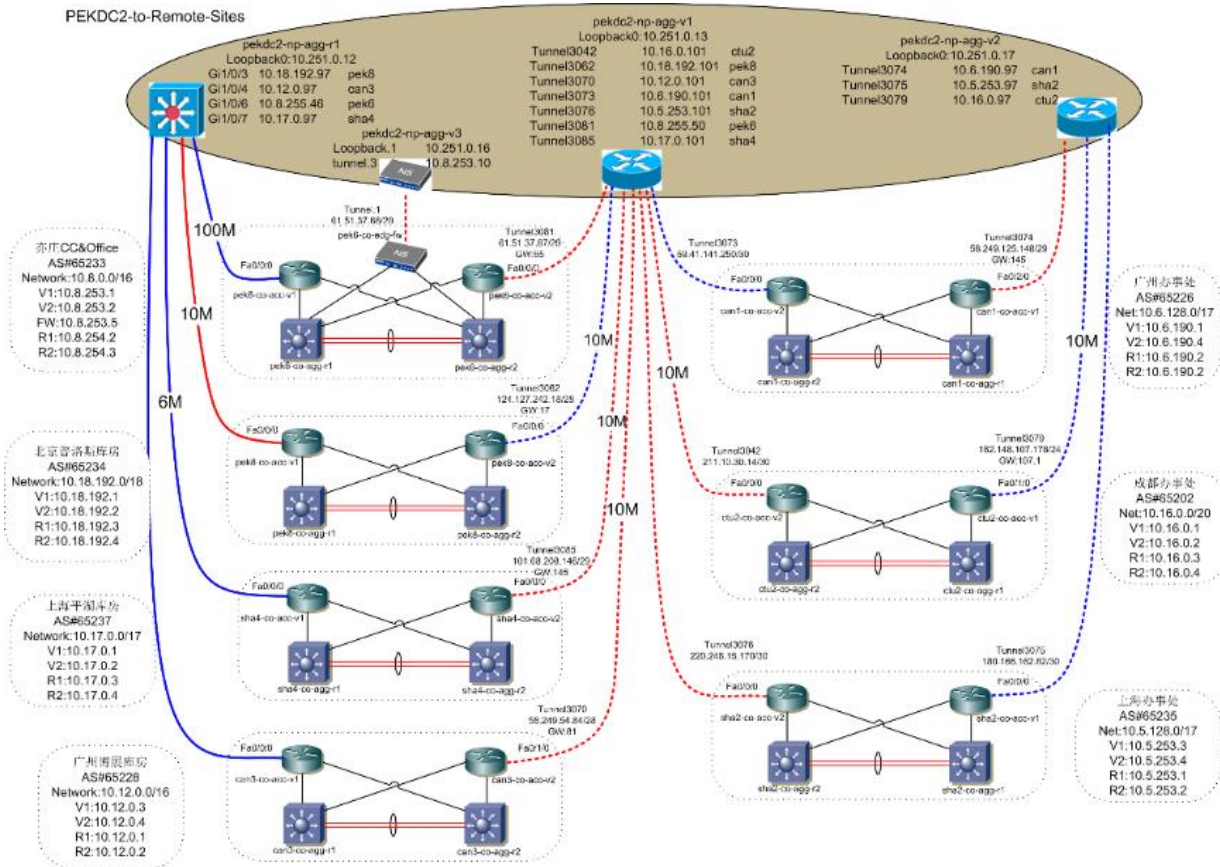
网络层之IDC

-

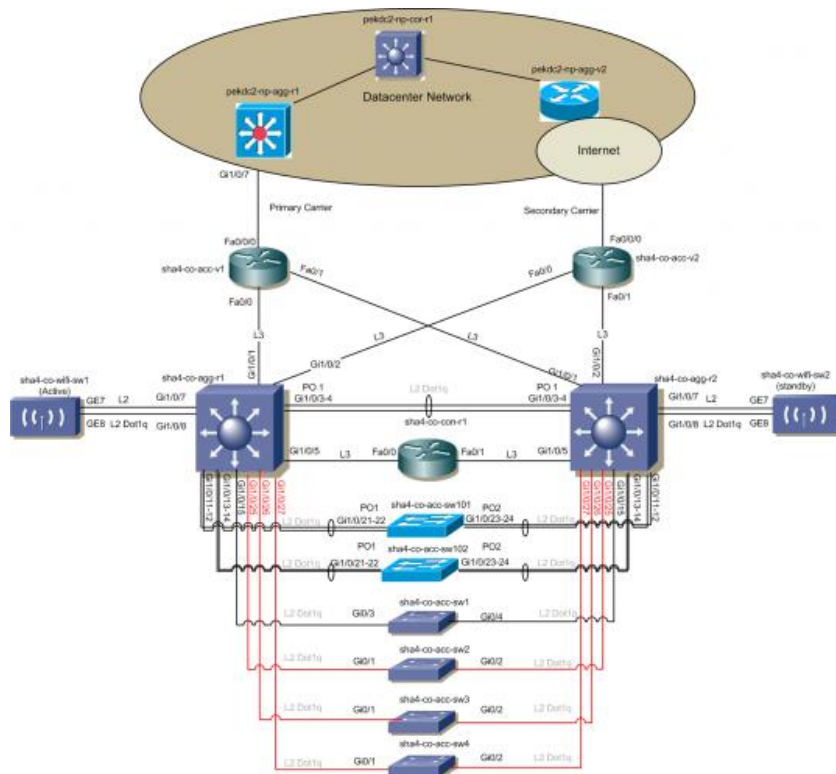


网络层之站点间

PEKDC2-to-Remote-Sites



网络层之站点内



LAYER 2 NETWORK

Access Layer:

(sha4-co-acc-sw) 使用 Fa0/39-48 连接 AP300, 其他端口连接 MDF PCs, 桌面客户端PC和IP电话. 每台接入交换机通过两个千兆电/光口分别上连到 sha4-co-agg-r[1-2].

Aggregate Layer:

2台sha4-co-agg-r[1-2]交换机将配置Dot1q port-channel去连接到Routers (sha4-co-acc-v[1-2]), 汇聚交换机通过光纤下连到接入交换机.

Transit Layer:

2台sha4-co-acc-v[1-2] routers使用三层去承载不同的流量.

生成树协议使用Rapid PVSTP, sha4-co-agg-r1是所有VLAN的根桥, sha4-co-agg-r2是备份根桥

VTP Domain 是vand, 两台agg-r交换机设置为服务器模式, 其交换机均是客户端模式.

汇聚层与接入层交换机链路均开启UDLD

VLAN Allocation:

- VPN Tunnel connection
- VLAN 801 Servers
- VLAN 802 Office Users
- VLAN 803 Voip
- VLAN 804 Production
- VLAN 806 RF-Scanner
- VLAN 807 TMG outside
- VLAN 808 Wifi Office Users
- VLAN 809 AP - non Routed
- VLAN 810 server console
- VLAN 888 Network Management

— Fiber
— Copper

主题: 中国联通sha4
创建人: 吕志宏
日期: 2013年11月20日



GOPS2016
Beijing

网络层之无线

- 办公和仓储
- 漫游和性能
- abng的选择
- 802.1X与网络验证



网络层之VPN

- 个人用户
- Site to site



网络层之QOS

- 基本都是双出口
- 业务流量优先
- 关键节点无单点
- 带宽监控
- 流量审计



网络层架构特点总结

- 网络的发展SDN
- 网络运维自动化
- 动态路由协议BGP、OSPF
- 网络质量控制QOS



机房层

- 场地、温湿度、电力、空调、机柜、承重、互联线路
- 站点自建
- IDC租赁



资源管理和监控

- 了解你跨下的宝马or自行车



安全与审计

- 纵深的安全机制
- 应用系统网络各个层面的安全意识深入骨髓



IT设计模型与实现



- 自顶向下
- 模块化



IT运维管理之贯彻“五化”

- 服务化
- 标准化
- 自动化
- 自助化
- 技术化（形成工具）



“五化”之IT服务化

- ITIL事件管理系统

▶ 系统首页	当前位置：系统首页					创建一个事件	搜
▶ 事件管理	SLA设置						
▶ 报表管理	万恶的SLA						
▶ 解决组管理	影响级别	响应时间	打开状态	等待状态	正在处理	已解决	
▼ 系统设置	1	24X7	15 分钟	15 分钟	90分钟	120分钟	
CTI设置	2	24X7	15 分钟	30 分钟	90分钟	120分钟	
SLA设置	3	BusinessHours	60 分钟	180 分钟	180分钟	240分钟	
	4	BusinessHours	120 分钟	360 分钟	360分钟	480分钟	
	5	BusinessHours	360 分钟	2160 分钟	2160分钟	2400分钟	



“五化”之IT服务自助化

你好,陈怡豪,欢迎使用账户管理系统 [我的信息](#) [密码修改](#) [编辑信息](#) [退出系统](#)

我的工作台

- 我管理的安全组
- 我管理的通讯组
- 我所属的组
- 我管理的账户
- 我的草稿箱(0)
- 我的申请单(30)
- 我进行中的(0)
- 等待我审批的(1)
- 我被拒绝的和撤销的(6)
- 我已完成的(24)
- 我审批过的(1808)
- 通知过我的(6924)

申请单创建

- 域账户申请单
- 安全组申请单
- 通讯组申请单
- 邮箱申请单
- 常用申请单

域对象管理

系统配置

当前位置: 域对象管理 [查询](#) [高级查询](#)

域对象管理

显示名	描述	对象操作
OA.ams.list	技术...通讯组	管理成员 管理员设置 修改 导出
IT.Support.list	技术支持...通讯组	续期 管理成员 管理员设置 修改 导出
phone.support.list	phone...技术支持组	续期 管理成员 管理员设置 修改 导出
技术...list	技术...通讯组	续期 管理成员 管理员设置 修改 导出
Portal.list	Portal...网...目团队	续期 管理成员 管理员设置 修改 导出
aes.list	aes...组	续期 管理成员 管理员设置 修改 导出
it.account.list	员工...信息将发往此组	续期 管理成员 管理员设置 修改 导出
OA.Password.list	新员工初始...该组	续期 管理成员 管理员设置 修改 导出
mailforfeedback.list	QQ使用...获取自己域名下的邮箱所发过...件被举报的信息	续期 管理成员 管理员设置 修改 导出
postmaster.list	postmaster...feedback开头的邮件地址,用于处理邮件投递反馈	续期 管理成员 管理员设置 修改 导出
Allow market.list	允许此组成员可以...邮件给market.list	续期 管理成员 管理员设置 修改 导出
Observation.account.list	用于接收重点...密码过期提醒的邮件组	续期 管理成员 管理员设置 修改 导出
Qa.net.list	...	续期 管理成员 管理员设置 修改 导出
IT.Engineering.list	IT...程师组	续期 管理成员 管理员设置 修改 导出
技术系统...项目	产...链系统项目	续期 管理成员 管理员设置 修改 导出
IDC...团队	IDC...队	续期 管理成员 管理员设置 修改 导出
IT.Ne...组	...通讯组	续期 管理成员 管理员设置 修改 导出



“五化”之IT自动化

你好,陈貽泰,欢迎使用账户管理系统 [我的信息](#) [密码修改](#) [编辑信息](#) [退出系统](#)

当前位置: 域对象管理

[启用邮箱](#)

* 部门名: * 创建日期: 2012-25

[查询](#) [启用邮箱](#)

<input type="checkbox"/>	姓名	域账户	部门	职位	最后更新时间
<input type="checkbox"/>	赵		VJIA事业部-开发三组	技术开发工程师	2012/6 17:34:00
<input type="checkbox"/>	陈	chenh	市场推广部-市场管理部	数据分析专员	2012/6 16:46:00
<input type="checkbox"/>	张	zha	废拣运中心-废上海分拣部	发货员	2012/6 16:13:00
<input type="checkbox"/>	赵	zha	营销策划组-摄影组	摄影师	2012/10 11:28:46
<input type="checkbox"/>	王	wan	质检中心-上海质检部	质检员	2012/7/6 11:28:46

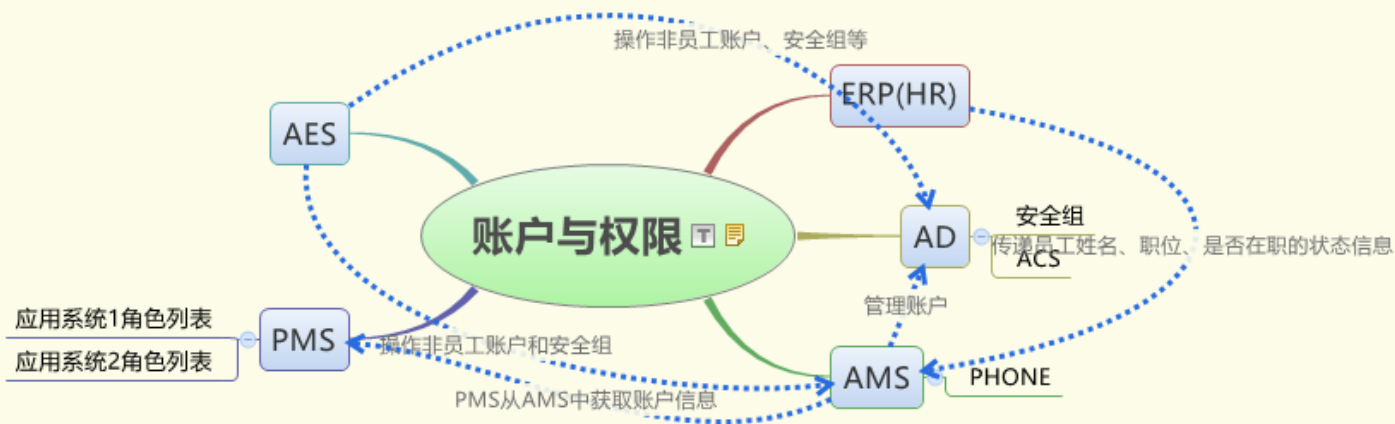
[首页](#) [上一页](#) [1](#) [下一页](#) [末页](#)

- 域账户申请单
- 安全组申请单
- 通讯组申请单
- 邮箱申请单
- 常用申请单
- 域对象管理**
 - 员工账户
 - 非员工账户
 - 计算机
 - 安全组
 - 组织单元
 - 通讯组
 - 批量启用员工邮箱**
 - 员工密码修改查询
 - 锁定账户查询

系统配置



“五化”之账户管理自动化



“五化”之其他

- 标准化
- 技术化

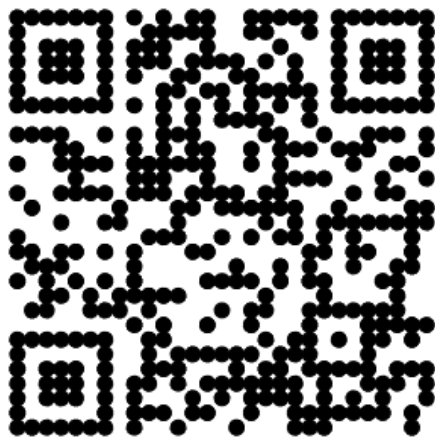


DevOpsDays 即将首次登陆中国



DevOps 之父 Patrick Debois 与您相约

DevOpsDays 北京站 2017年3月18日



门票早鸟价仅限前100名，请从速哟

<http://2017-beijing.devopsdayschina.org/>



GOPS2016
Beijing



想第一时间看到
高效运维社区公众号
的好文章吗？

请打开高效运维社区公众号，点击右上角小人，如右侧所示设置就好





Thanks

高效运维社区
开放运维联盟

荣誉出品

