联想网御

助力高校应用，保障数字校园

万兆校园网络安全解决方案

李江力
联想网御科技（北京）有限公司

lenovo

高校校园网发展历程


1994-2000
网络技术
10Base-5以太网
10/100M以太网
FDDI /ATM
关注要点
连通
兼容
2000-2005
网络技术
千兆以太网
三层交换技术
防火墙
关注要点
带宽
应用
2005-至今
网络技术
10G/40G以太网
100G以太网
IPv6
关注要点
校务与IT的深度结合
校务保障
……

高校校园网安全现状


仿冒DHCP
ARP攻击
宿舍区网络
篡改
IP/MAC
……
校园数据中心
……
发布发
动言论
邮件附件
带毒
DDOS
攻击
出口链
路备份
Cernet/Internet
链路负载
分担
P2P带
宽滥用
网页带毒
色情网站
……
远程接入校
园网
教学科研办
公区网络
补丁不全
未装杀毒
软件
越权访问
……

万兆网络安全解决方案

校园网出口安全

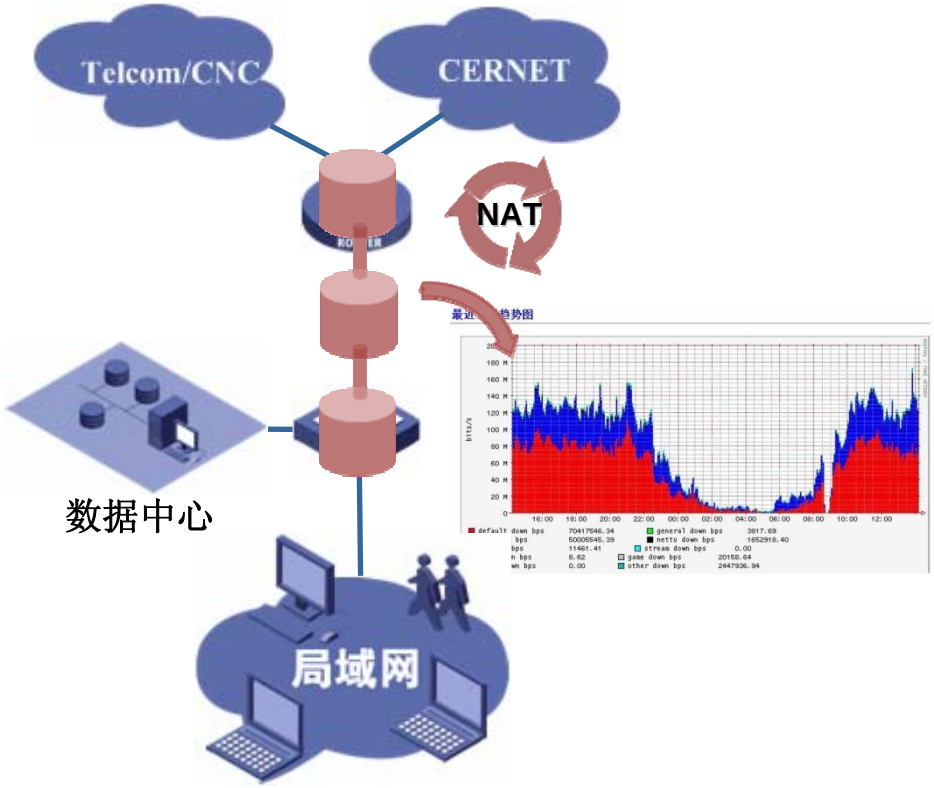
校园网应用安全

安全方案之

校园网出口安全

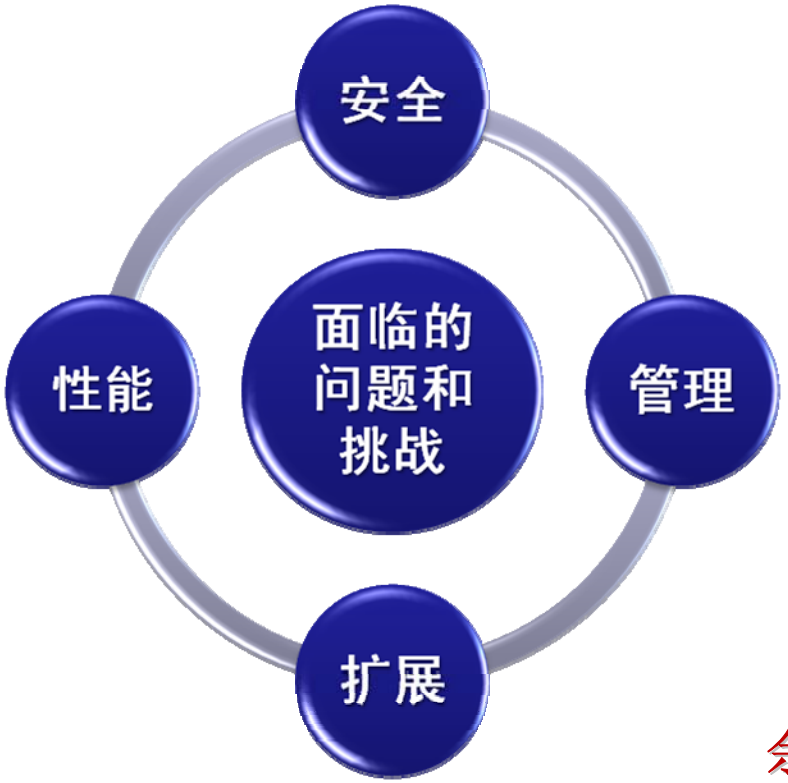
- 出口特点
- 面临问题
- 解决方案
- 用户价值

校园网出口特点



- 两个或多个出口
- 存在大量的地址转换
- 出口流量巨大，具有突发性
- P2P、网络电视流量比例高
- 出口带宽扩展比较频繁

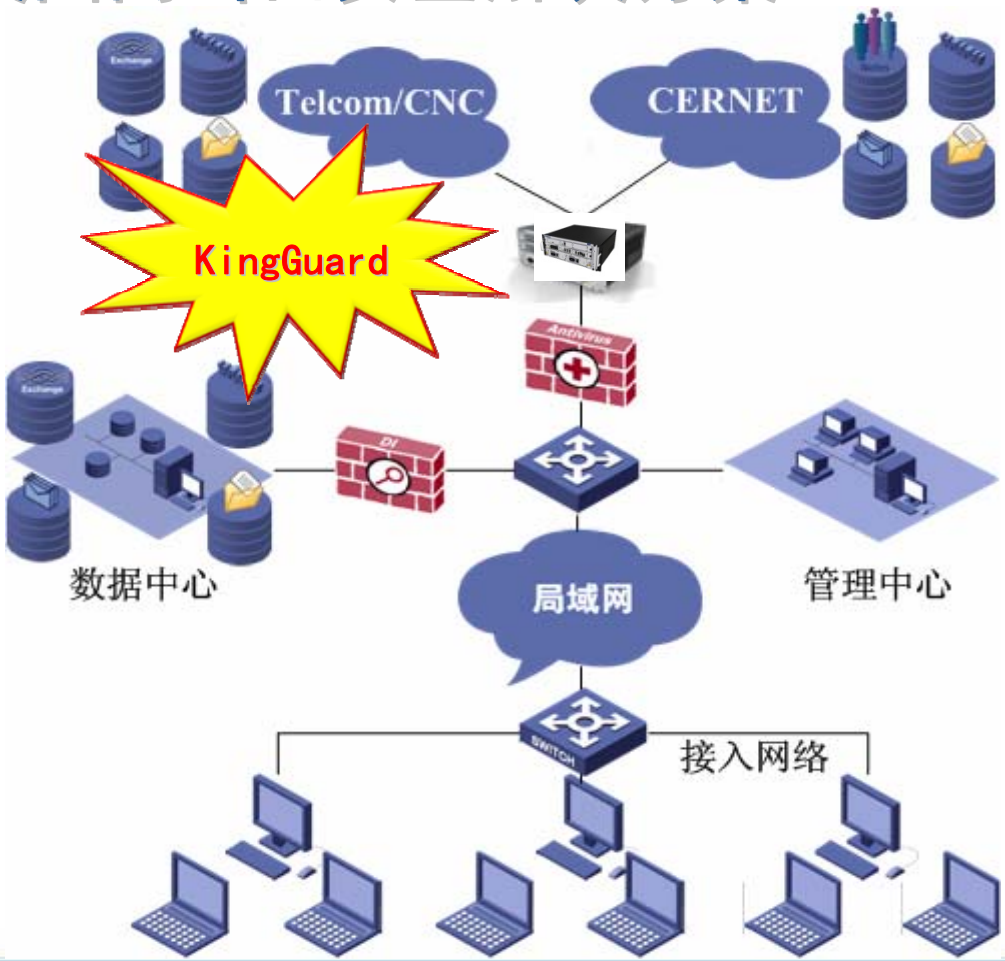
面临的问题和挑战



- 出口设备性能不够！
- 出口链路可靠性不够!
- 出口安全性不够！
- 出口带宽总是紧张！
- 未来2-3年的可扩展性不够！

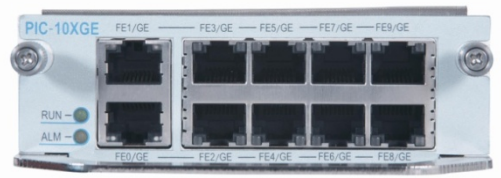
如何建设一个多出口负载分担、冗余备份的高性能高安全的网络出口呢？

校园网出口安全解决方案

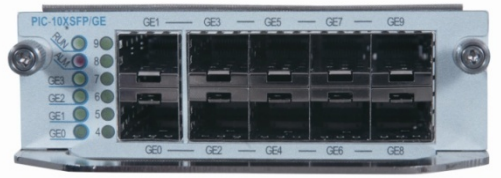


- 满足出口设备高性能要求
  - 高并发连接数
  - 高新建连接数
  - 大量NAT处理

灵活丰富的接口设计



PIC 10×GE



PIC 10×SFP

PIC 1×10XFP

满足出口设备多接口要求

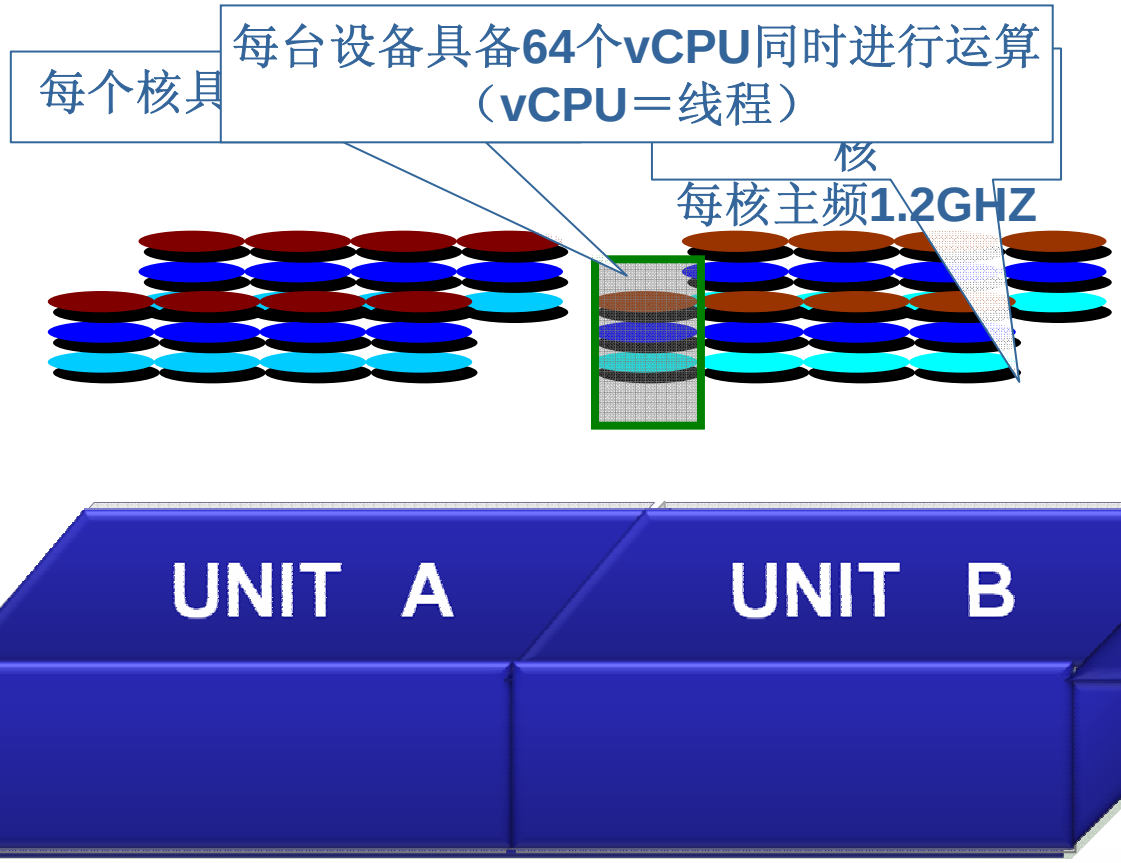
最多可以支持**4**万兆**XFP**光口

或**48**个千兆口

可满足用户不断升级的接口需求

吞吐：**20G**
并发：**500**万
每秒新建：**20**万

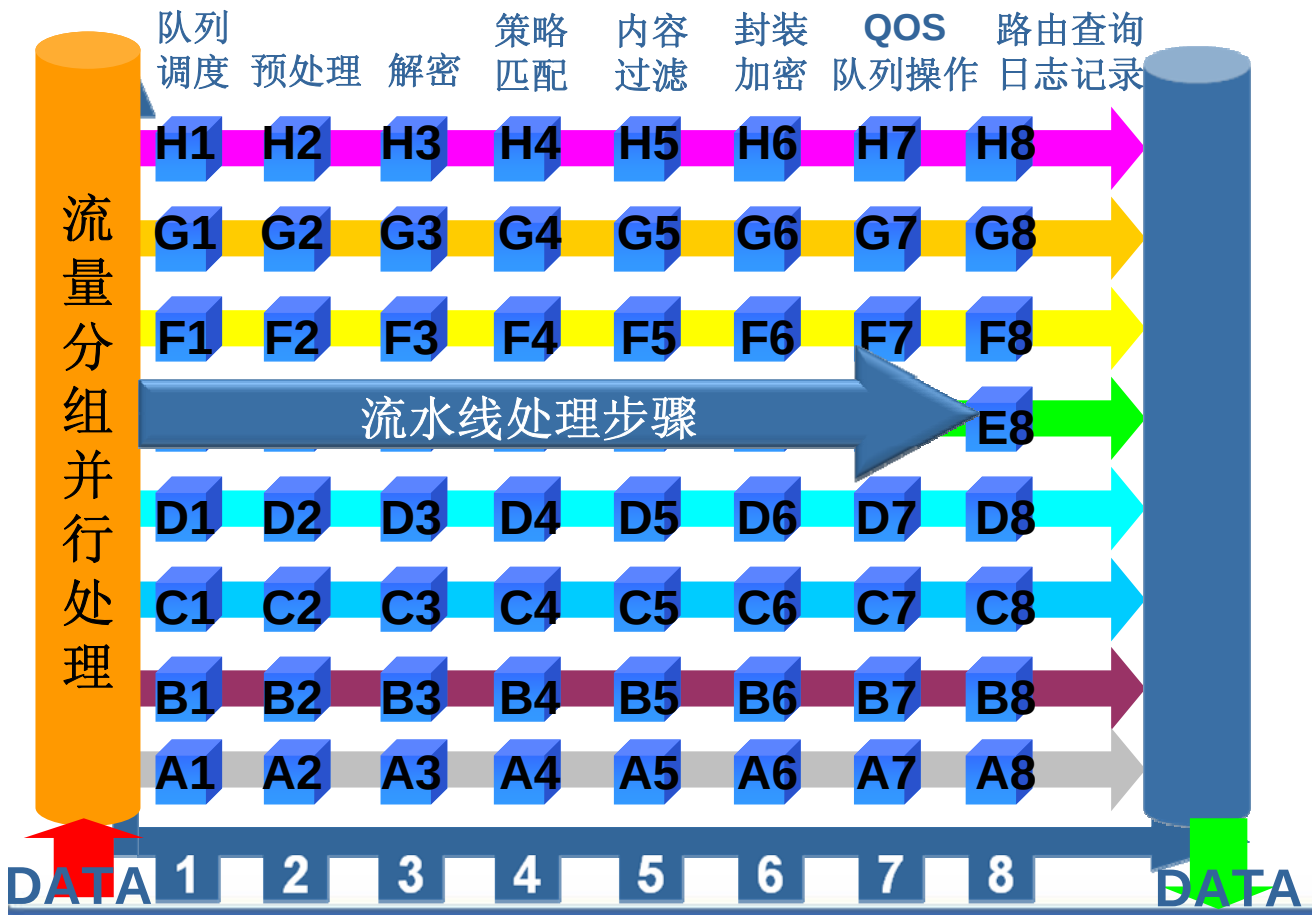
满足出口设备高性能要求－KingGuard内核技术



吞吐：20G
并发：500万
每秒新建：20万

- 64个vCPU
- 8×8矩阵式并行处理系统
- 智能的vCPU调度系统Windrunner

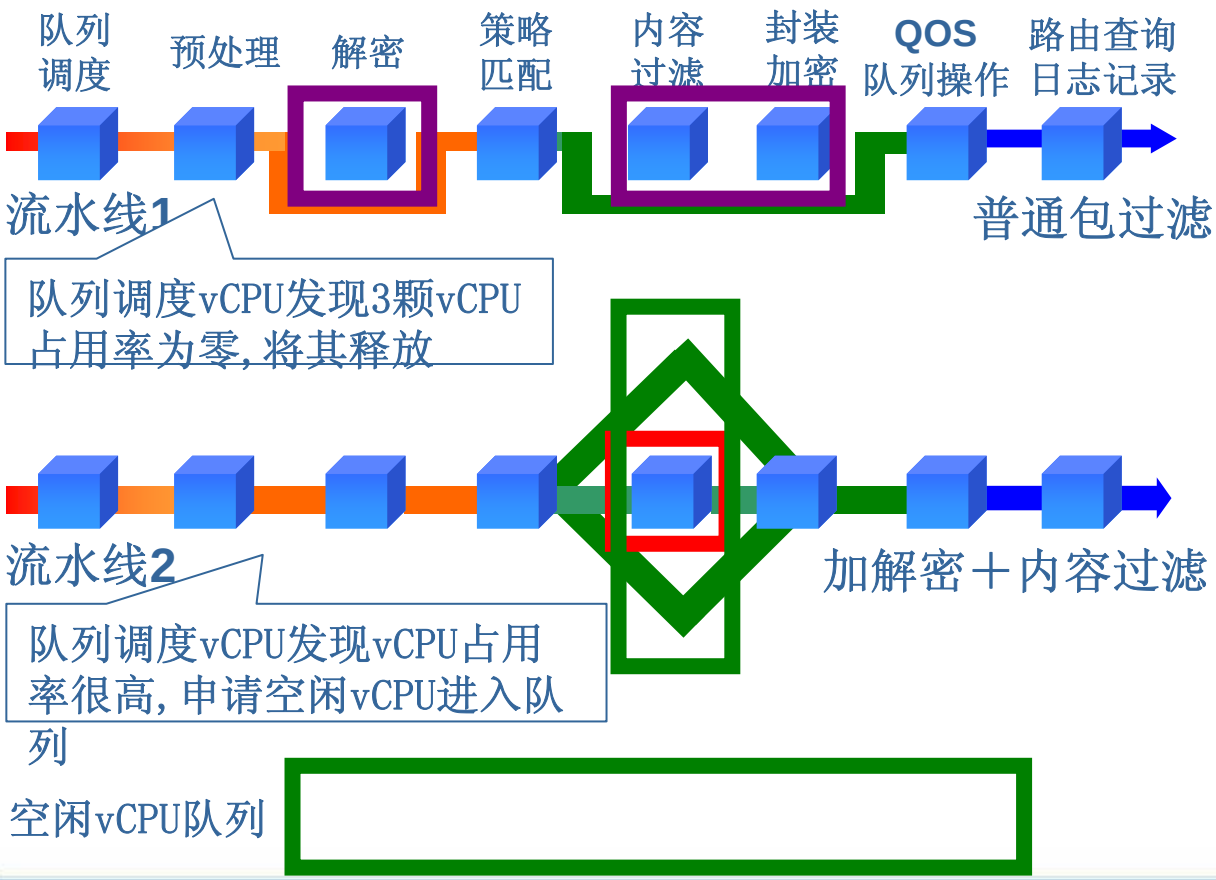
满足出口设备高性能要求－KingGuard内核技术



吞吐：20G
并发：500万
每秒新建：20万

- 64个vCPU
- 8×8矩阵式并行处理系统
- 智能的vCPU调度系统Windrunner

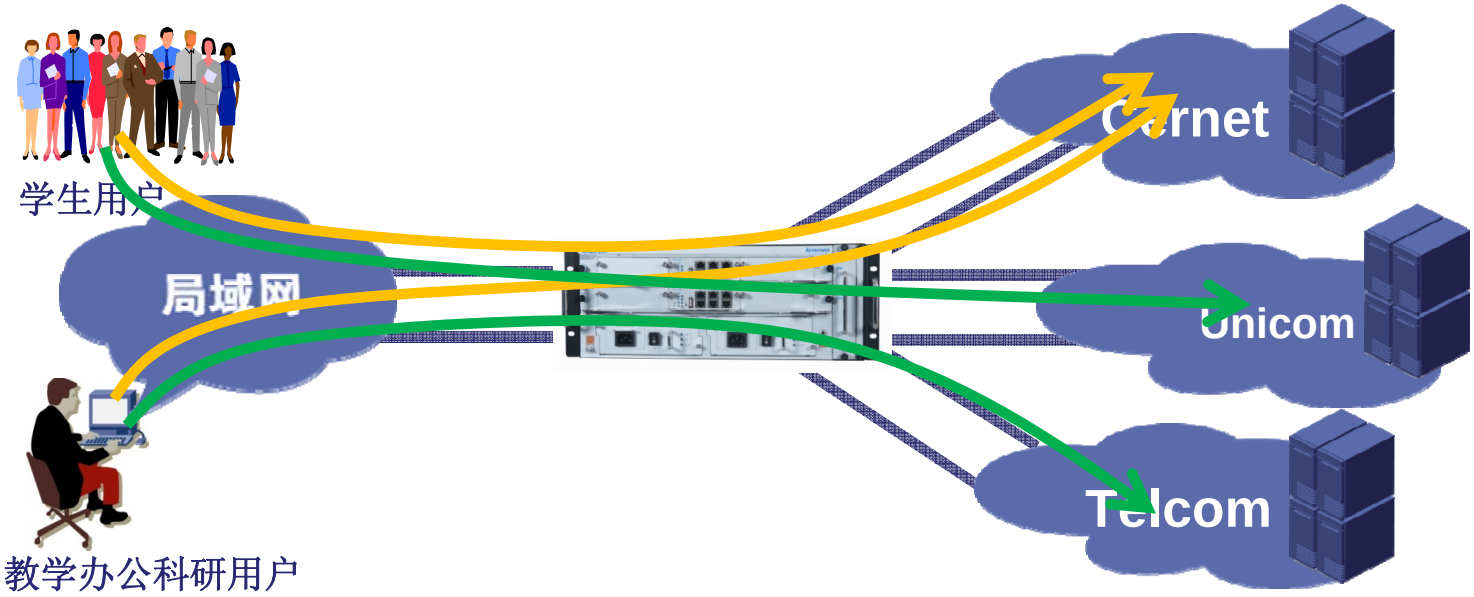
满足出口设备高性能要求－KingGuard内核技术



吞吐：20G
并发：500万
每秒新建：20万

- 64个vCPU
- 8×8矩阵式并行处理系统
- 智能的vCPU调度系统Windrunner

校园网多出口选择设计



学生用户访问教育网资源

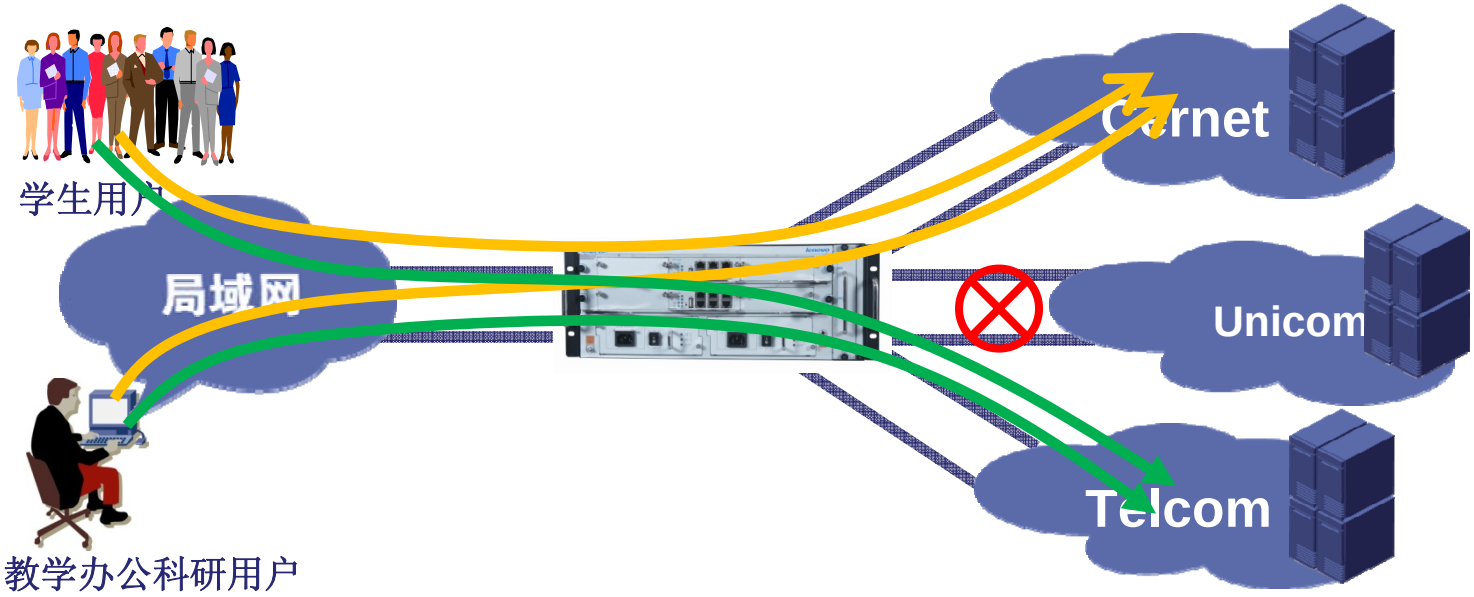
教学办公科研用户访问教育网资源

学生用户访问Internet资源

教学办公科研用户访问Internet资源

负载分担

校园网多出口互备设计



学生用户访问教育网资源

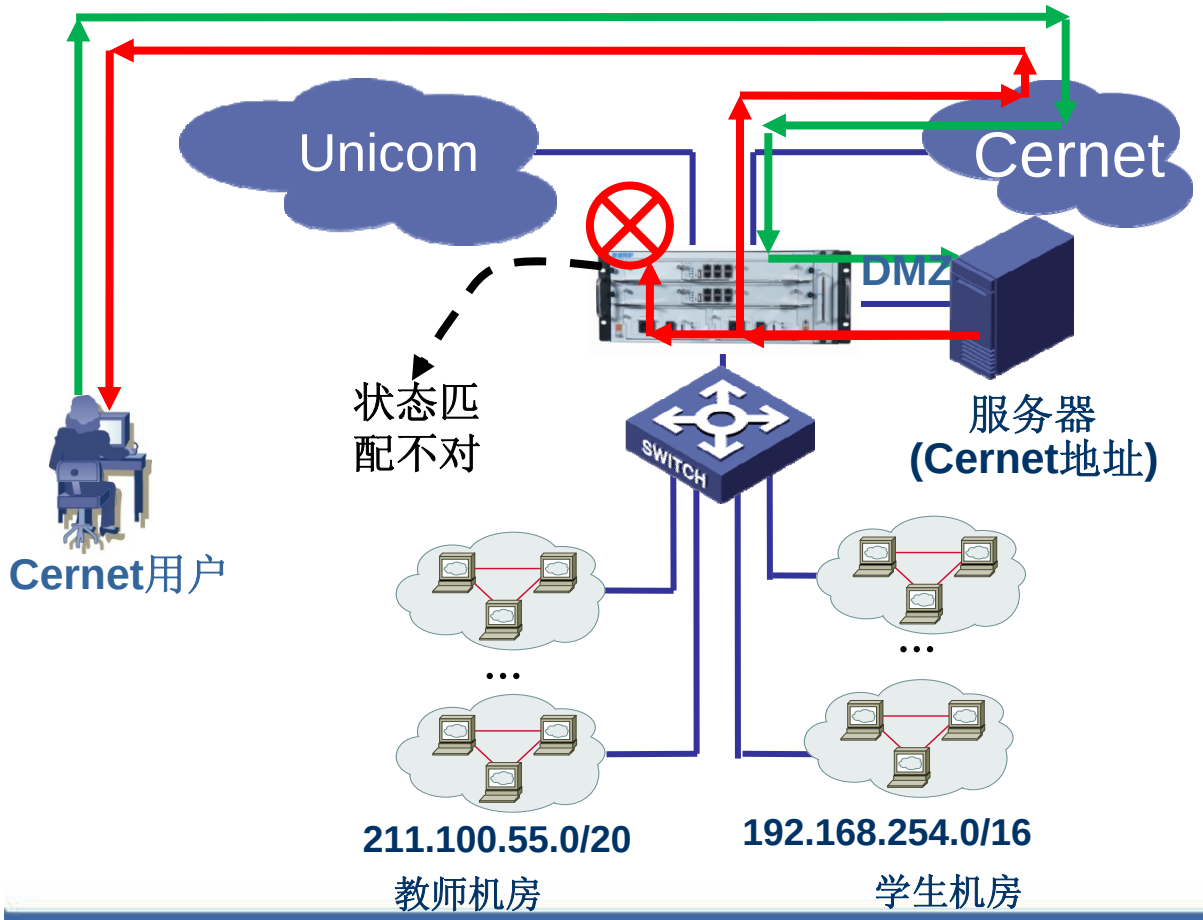
教学办公科研用户访问教育网资源

学生用户访问Internet资源

教学办公科研用户访问Internet资源

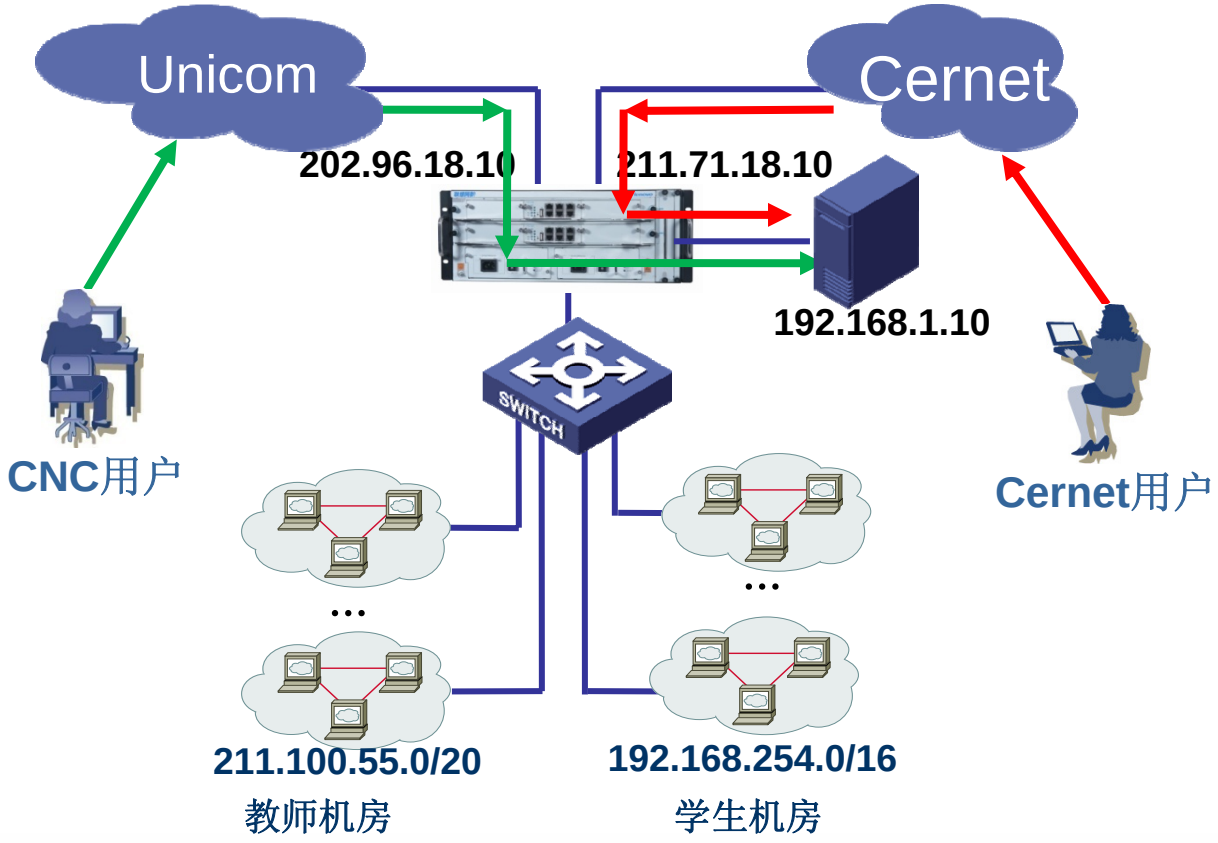
冗余备份

多ISP接入时智能路由选择设计



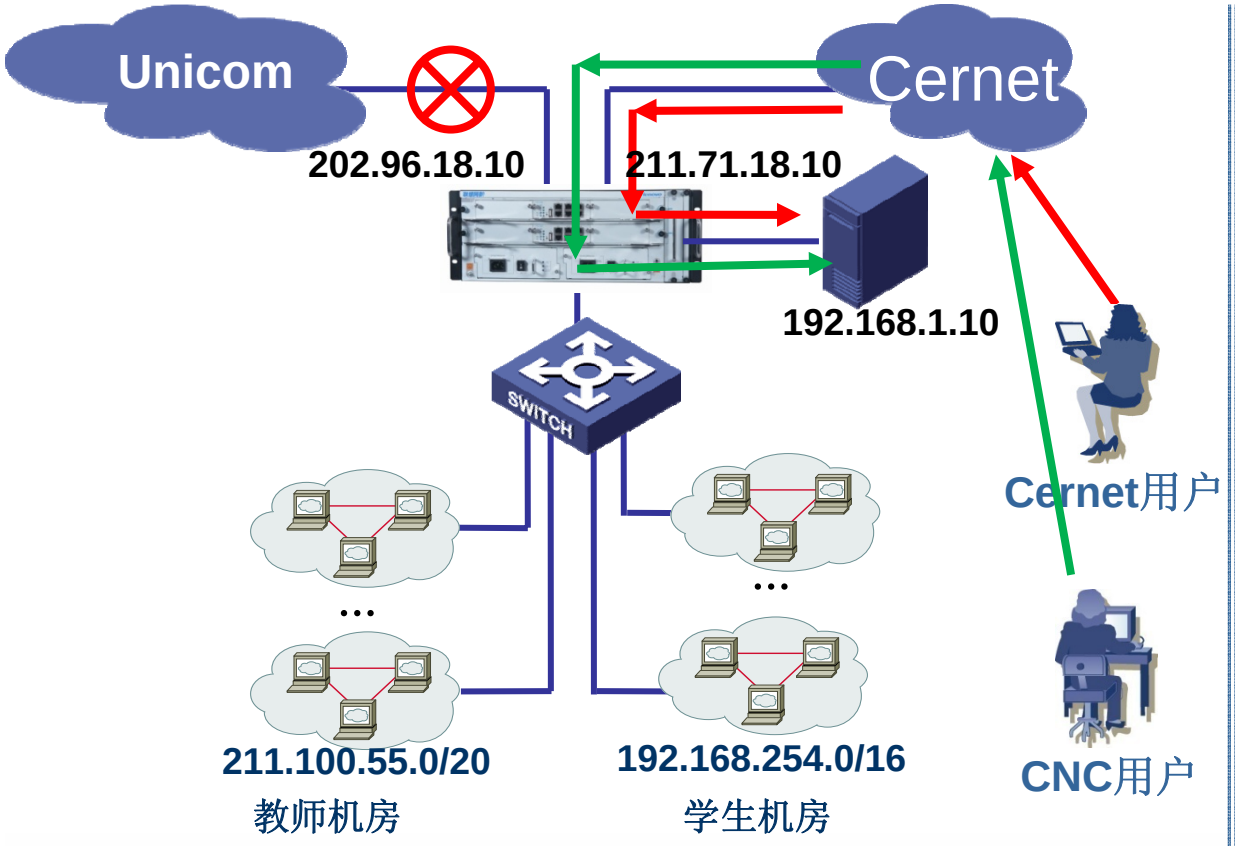
有效规避访问数据包和返回数据包走不同接口的问题

服务器多地址互为备份设计



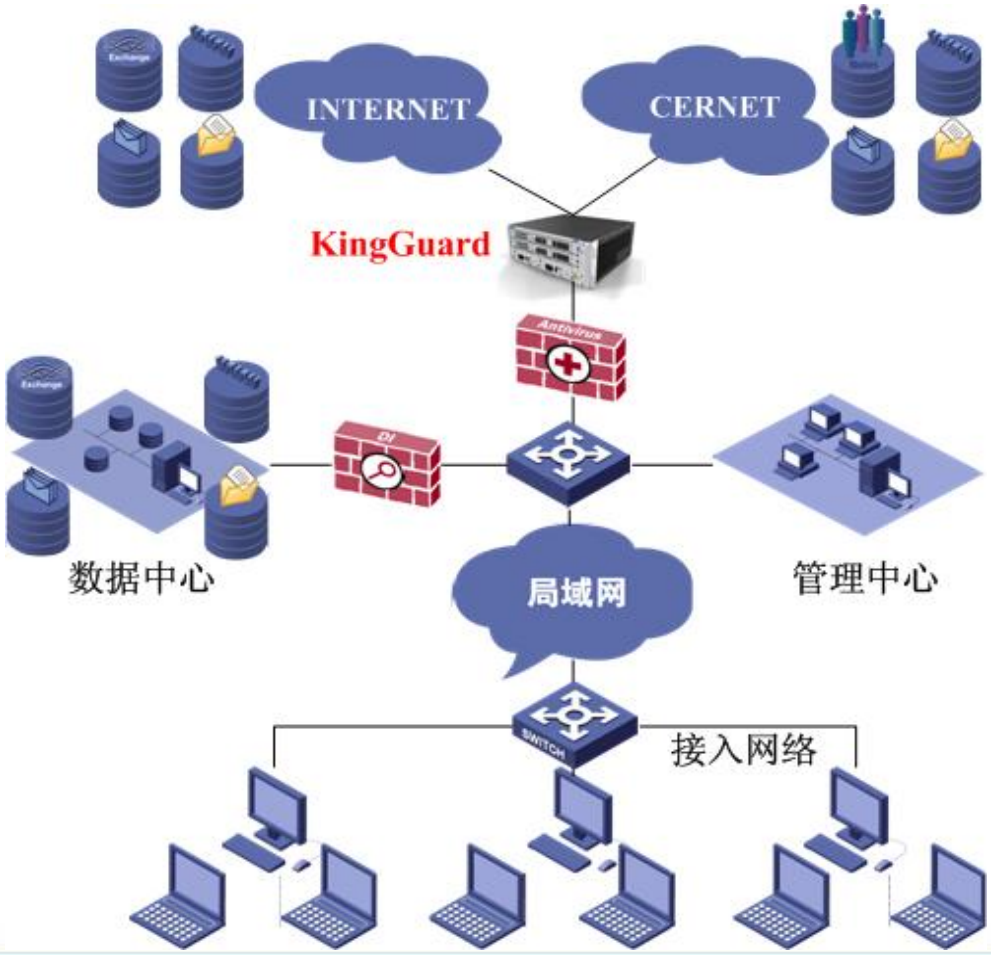
- 服务器使用一个私有地址
- 在KingGuard外网口上分别对应Unicom地址和Cernet地址
- 正常情况下，Cernet用户访问Cernet地址，Unicom用户访问Unicom地址

服务器多地址互为备份设计



- 可以有效解决服务器的Cernet和Unicom地址互为备份
  - 当Unicom链路中断时候，所有用户可通过Cernet地址访问服务器
  - 当Cernet链路中断时候，所有用户可通过CNC地址访问服务器

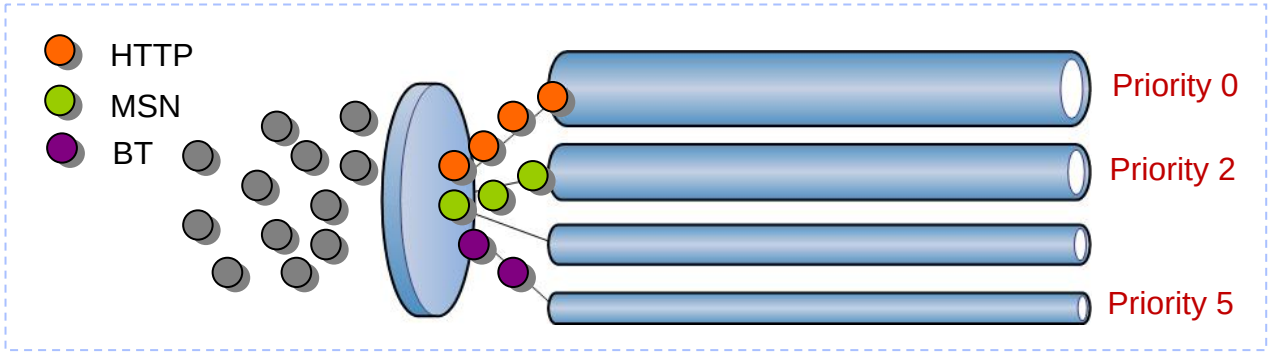
用户网络行为管控—切入点



- 校园网出口层
  - 网络访问去向集中的关口
  - **上网行为的关键路径**
- 校园网接入层
  - 产生网络行为的始发站

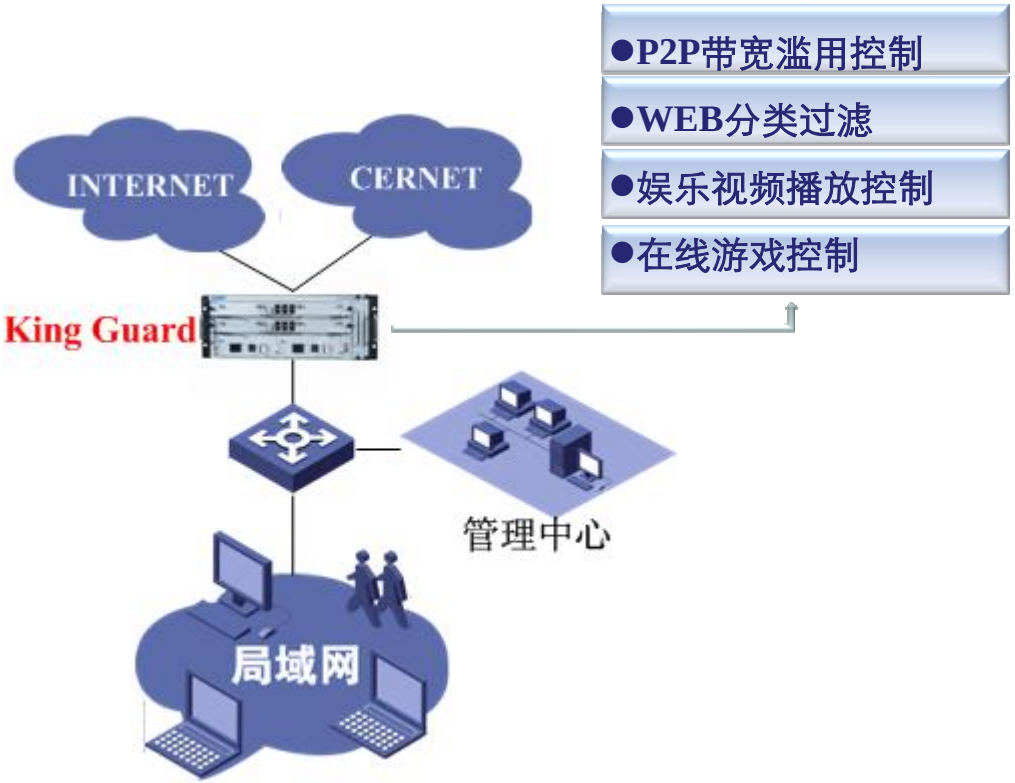
用户网络行为管控—方法

根据校园网用户需求对应用划分通道



- 支持基于用户、时间段、应用协议的带宽分配管理策略
- 支持自定义带宽通道，以及对应的优先级、速率上限和下限的设定

用户网络行为管控—实践



带宽控制策略

- 流量控制，总下行流量不得超过40Gb，超过后，带宽自动减为原来的1/3
- BIT、EM、迅雷等P2P工具总流量限制在100M以内
- PPLive、PPS、UUSee等在线电视总流量限制在80M内

KingGuard特点－超强性能

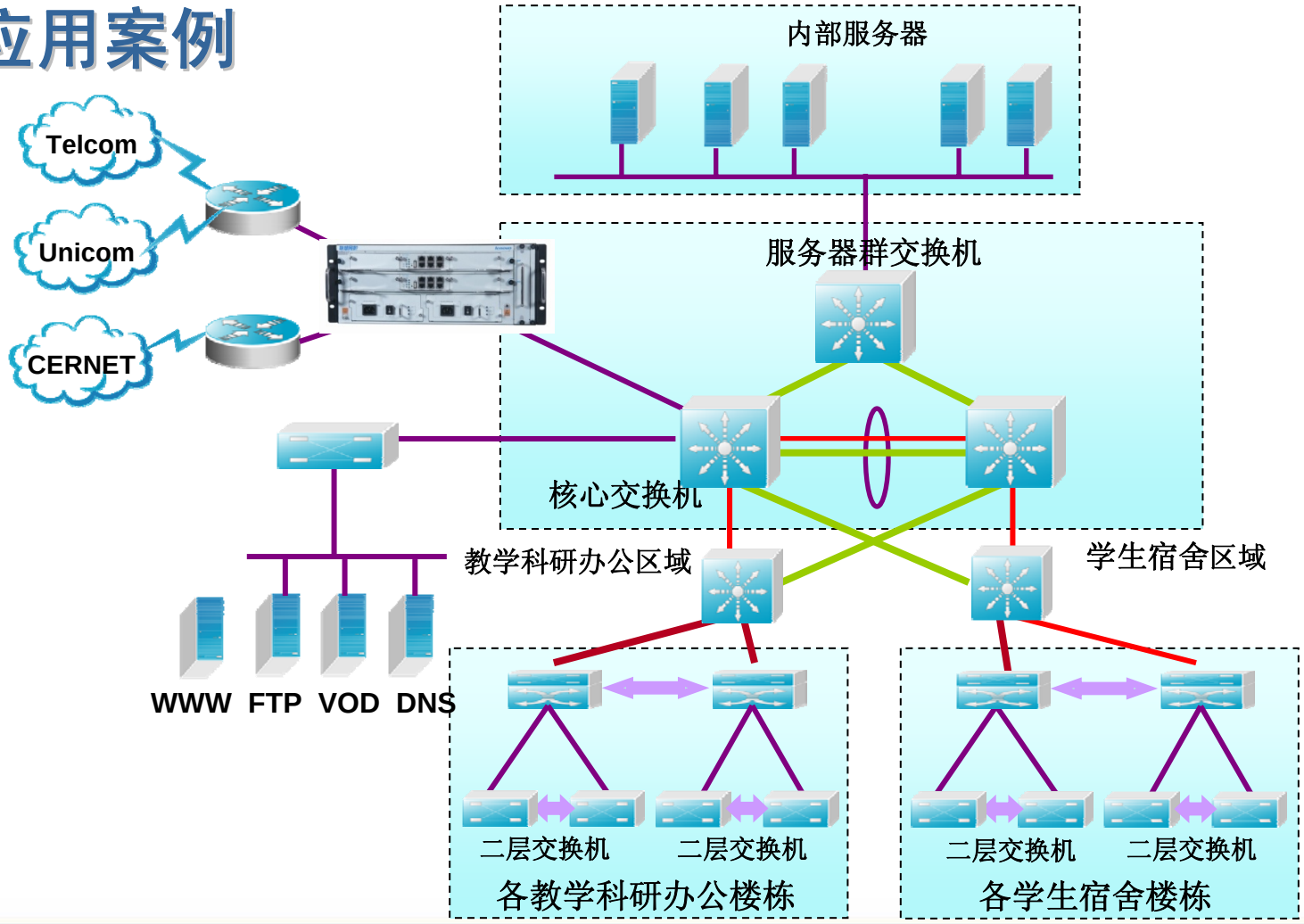
比较项	市场现有高端防火墙	KingGuard安全网关
处理能力	10－20G	20G
并发连接数	100－300万	500万（NAT后300万）
每秒新建连接	1.8－10万/秒	20万/秒（NAT后10万）
端口数目	支持48千兆口的厂家很少	最多可支持48个千兆口
可扩展性	大多数通过数据板扩展端口	可扩展数据板和端口模块,预留IPS/AV内容加速模块插槽

KingGuard特点－电信级设备高可靠性

用户价值

比较项	原有方案	KingGuard方案	投资回报指数
方案设计	部署多种设备 	部署KingGuard安全网关 	设备部署数量减少75%
设备性能	高端千兆设备 2-4Gbps	第二代万兆设备 10-40Gbps	提高5-10倍 满足未来2-3年平滑升级
安全管理	串行部署、独立管理	单一部署、单一管理	网络瘫痪几率降低75% 管理响应时间缩短75%
建设成本	总投资成本高	国产知名品牌，性价比好	建设成本降低50%
售后服务	需要协调多个设备厂商，服务不及时	30多个分支机构保障本地化服务	保障已有安全投入

应用案例


内部服务器
Telcom
Unicom
CERNET
服务器群交换机
核心交换机
教学科研办公区域
学生宿舍区域
WWW
FTP
VOD
DNS
二层交换机
二层交换机
各教学科研办公楼栋
二层交换机
二层交换机
各学生宿舍楼栋

教育行业主推产品

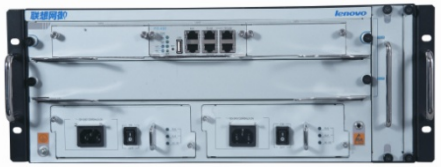
3万用户规模学校

5万用户规模学校

8万用户规模学校

KingGuard－8000

- 20 Gbps吞吐量
- 5,000,000个并发连接数
- 200,000每秒新建连接数
- 3 Gbps VPN吞吐量
- 10,000个VPN隧道数
- 可扩展至24个千兆端口或2个XFP万兆端口加4个千兆端口
- 多核架构



KingGuard－9201

- 20 Gbps吞吐量
- 5,000,000个并发连接数
- 200,000每秒新建连接数
- 3 Gbps VPN吞吐量
- 10,000个VPN隧道数
- 可扩展至48个千兆端口或4个XFP万兆端口加8个千兆端口
- 多核架构

KingGuard－9202

- 40 Gbps吞吐量
- 10,000,000个并发连接数
- 400,000每秒新建连接数
- 6 Gbps VPN吞吐量
- 10,000个VPN隧道数
- 可扩展至48个千兆端口或4个XFP万兆端口加8个千兆端口
- 多核架构

用户案例

青岛政务网 WWW.QINGDAO.GOV.CN

北京市国家保密局 Beijing State Secrecy Bureau

中南财经政法大学 Zhongnan University of Economics and Law

广东工业大学 Guangdong University of Technology

浙江审计 WWW.ZJSJT.GOV.CN SJT.ZJ.GOV.CN

东莞教育

武汉理工大学

东莞信息网 www.dgb2b.net

东莞某银行

长春工程学院 Changchun Institute of Technology

淳安县政府信息公开网

中国桐乡 TONGXIANG CHINA

威海职业学院 威海市技术学院 WEIHAI VOCATIONAL COLLEGE

力高校应

肇庆学院 ZHAOQING UNIVERSITY

lenovo

安全方案之

数字校园应用安全

- 应用概况
- 安全需求
- 解决方案
- 用户价值

数字校园发展阶段

第一阶段	校园网基础设施建设
第二阶段	单项应用系统建设
第三阶段	各部门应用系统建设
第四阶段	学校综合资源信息系统建设

数字校园应用系统

共同困惑

- 走出校园如何安全使用？
- ……

共同特点

- 数字化资源
- **B/S**服务架构
- 网上在线服务
- 基于校园用户

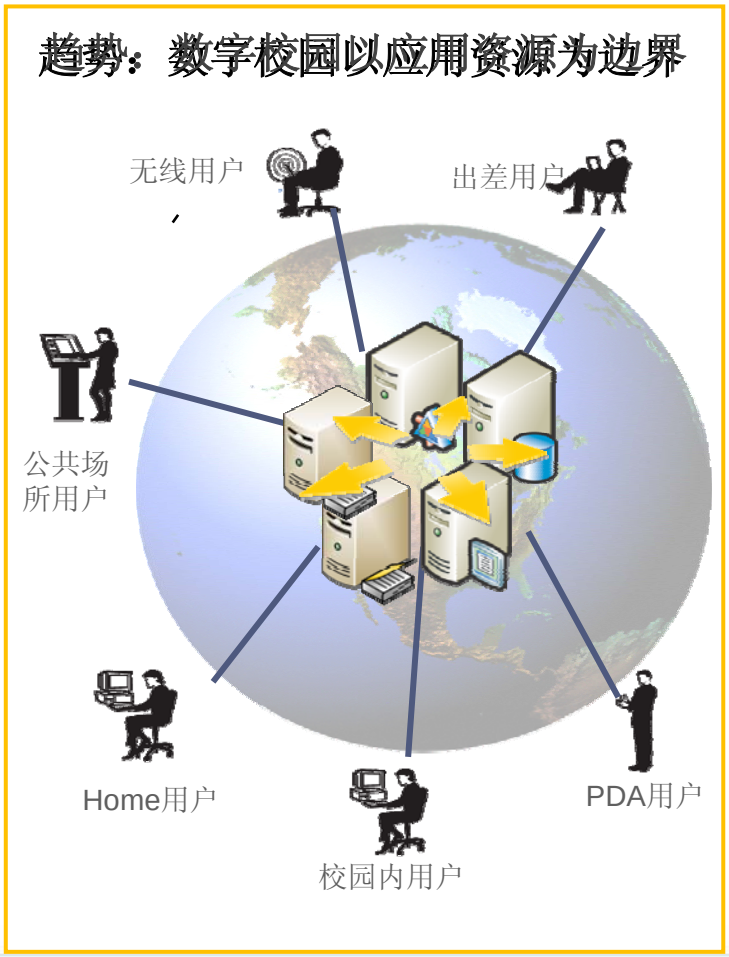
应用系统

- 数字图书馆
- 移动办公
- 网上选课
- 校务管理
- 网上财务
- 远程运维
- ……

真实的高校用户案例

为什么需要校外访问？而不仅仅是校内…

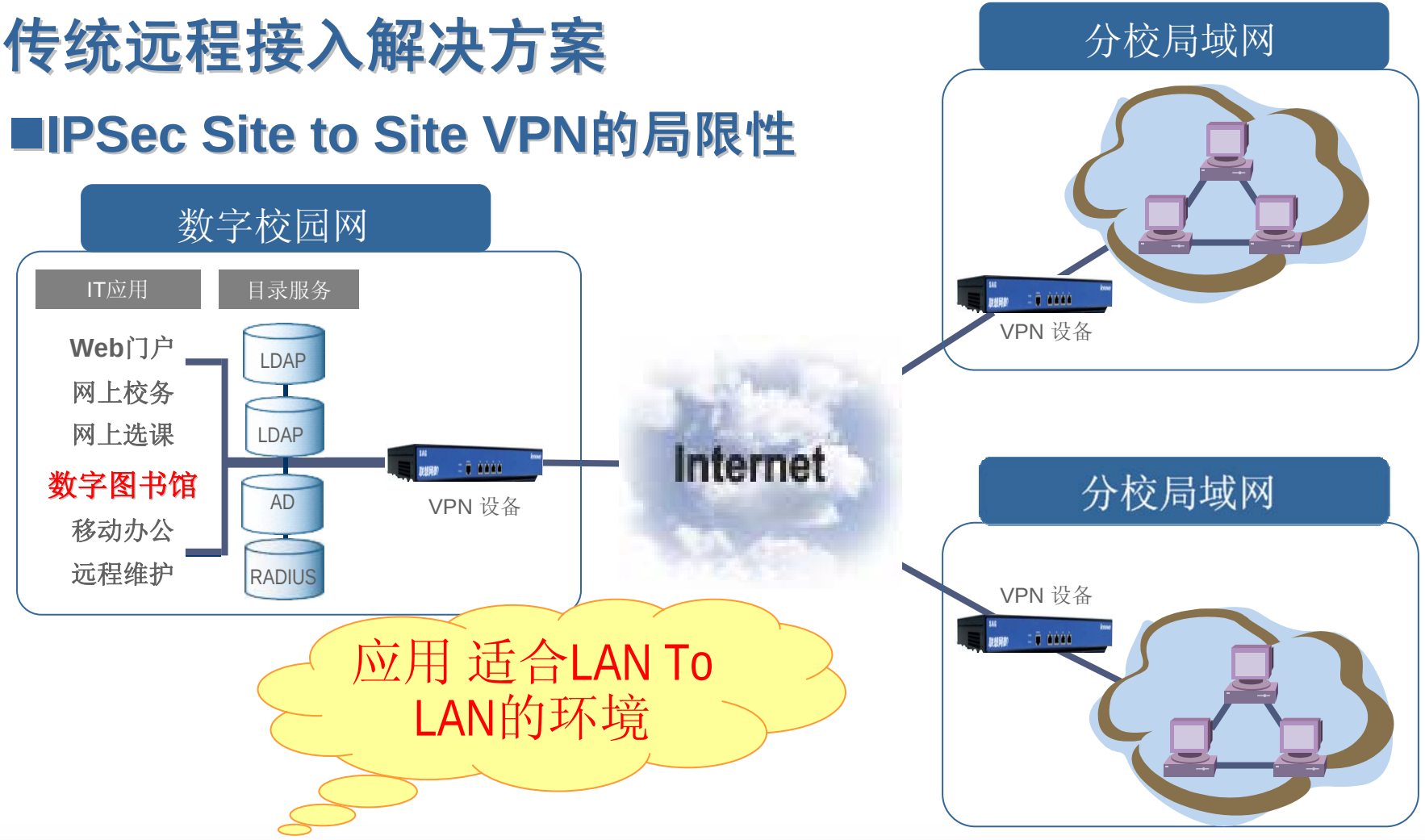
- 北京大学……
- 北京工商大学……



高校用户关注点是什么？

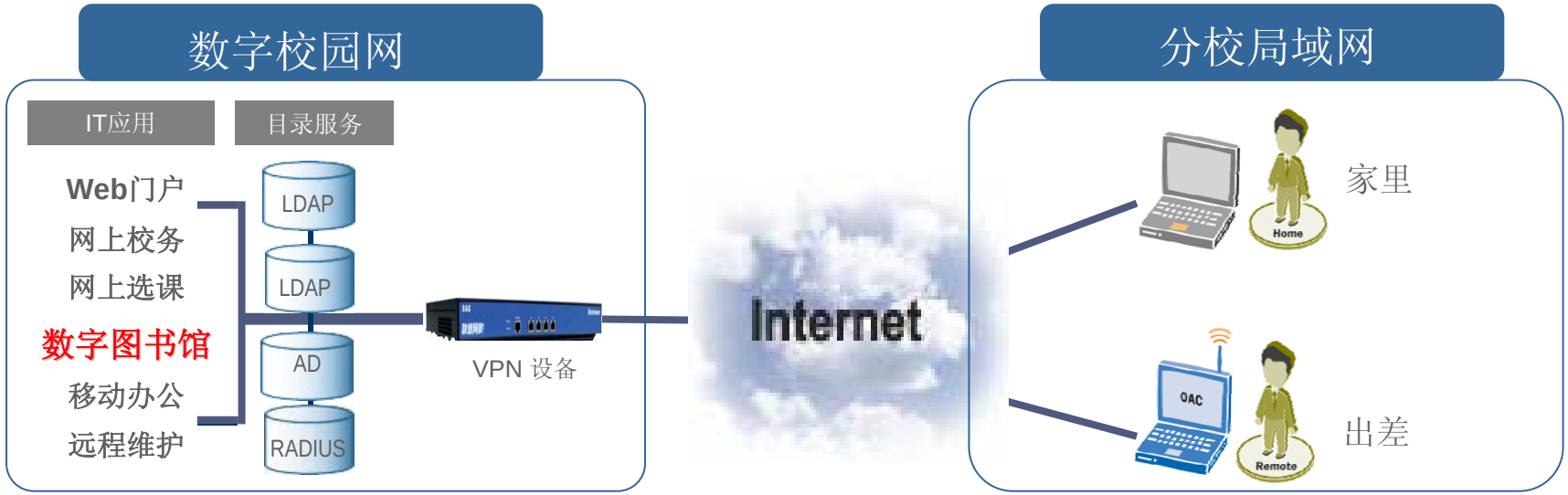
传统远程接入解决方案

■IPSec Site to Site VPN的局限性



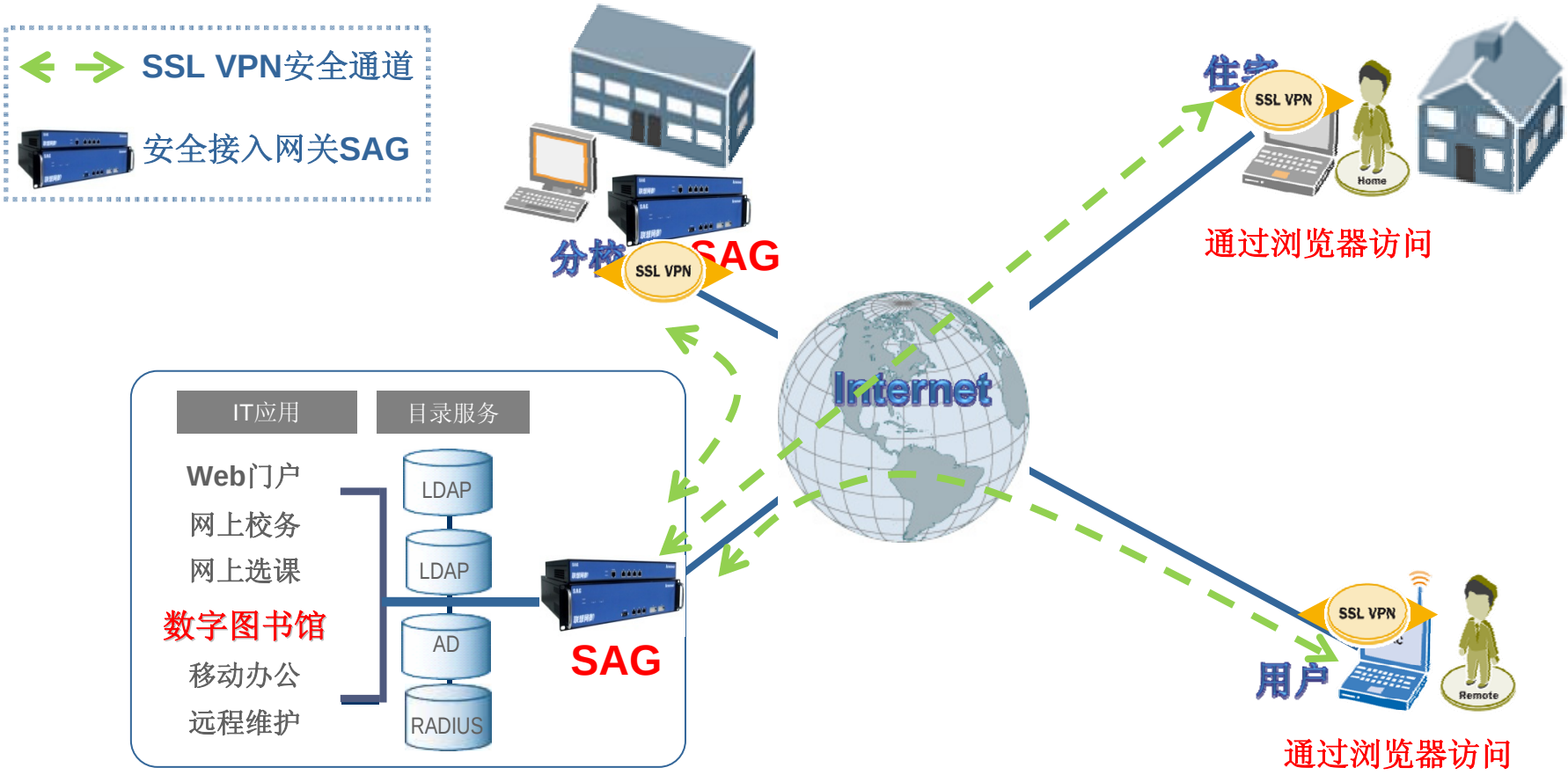
传统远程接入解决方案

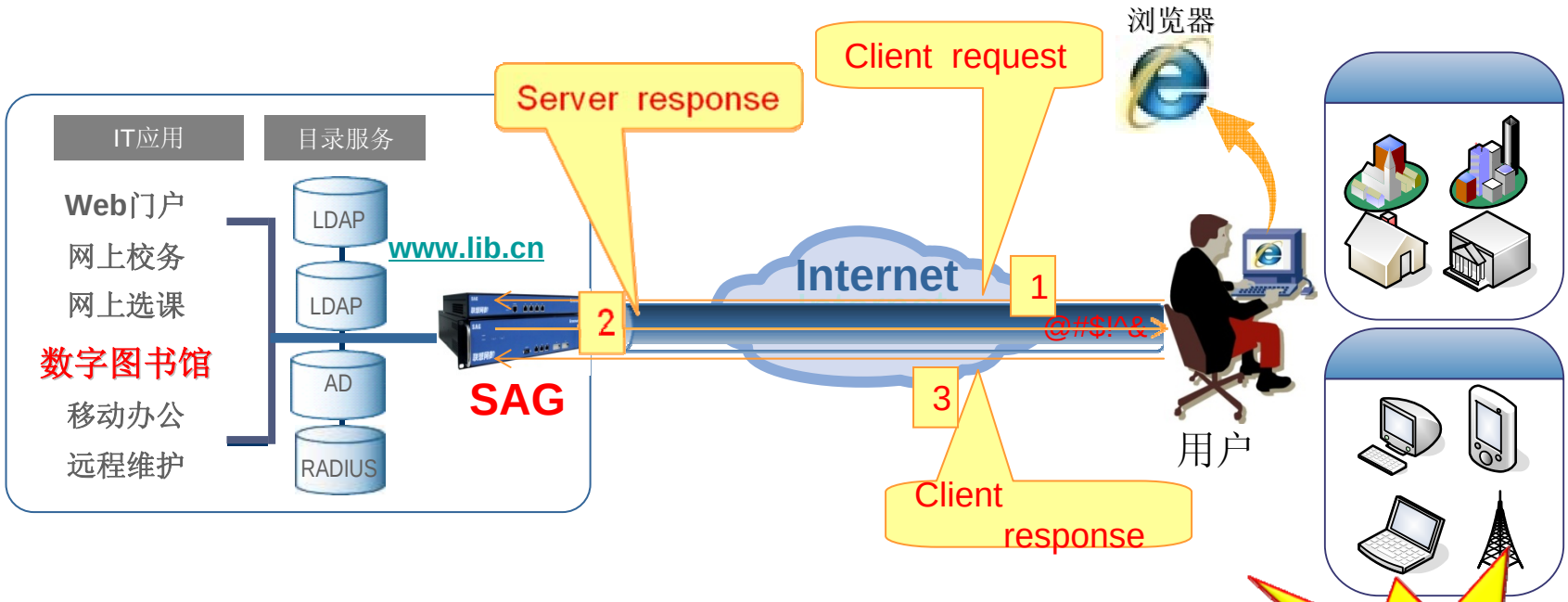
■IPSec Client to Site VPN的局限性



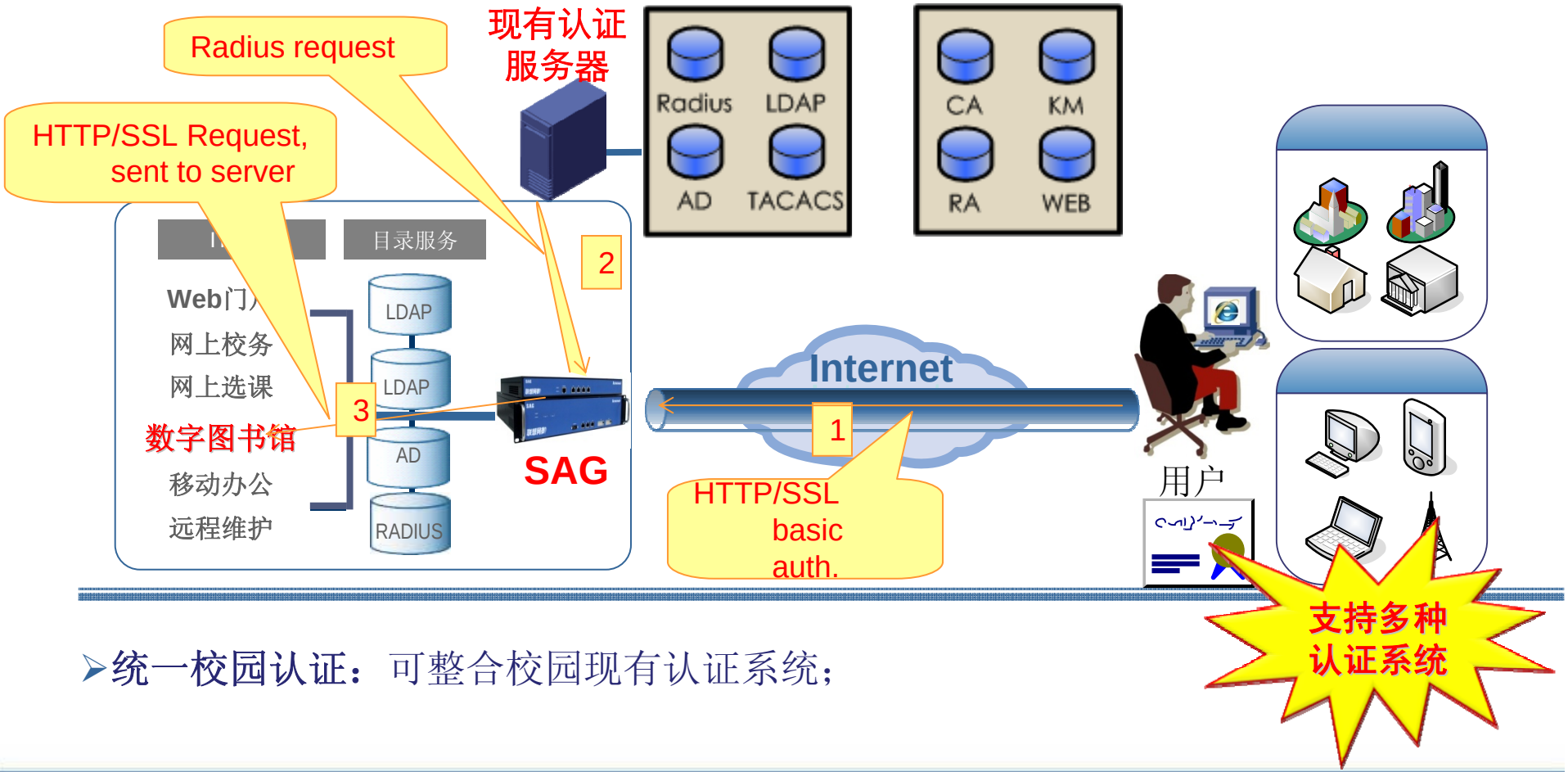
局限性: 1.便利性不够
2.手持设备支持
3.访问控制，身份识别问题
4.NAT 和防火墙穿越等技术问题

数字图书馆SSL VPN解决方案





- 符合安全标准：SAG遵循标准的SSL 协议，全面提供远程安全传输
- 加密通讯：可使攻击者不能了解、修改敏感信息；

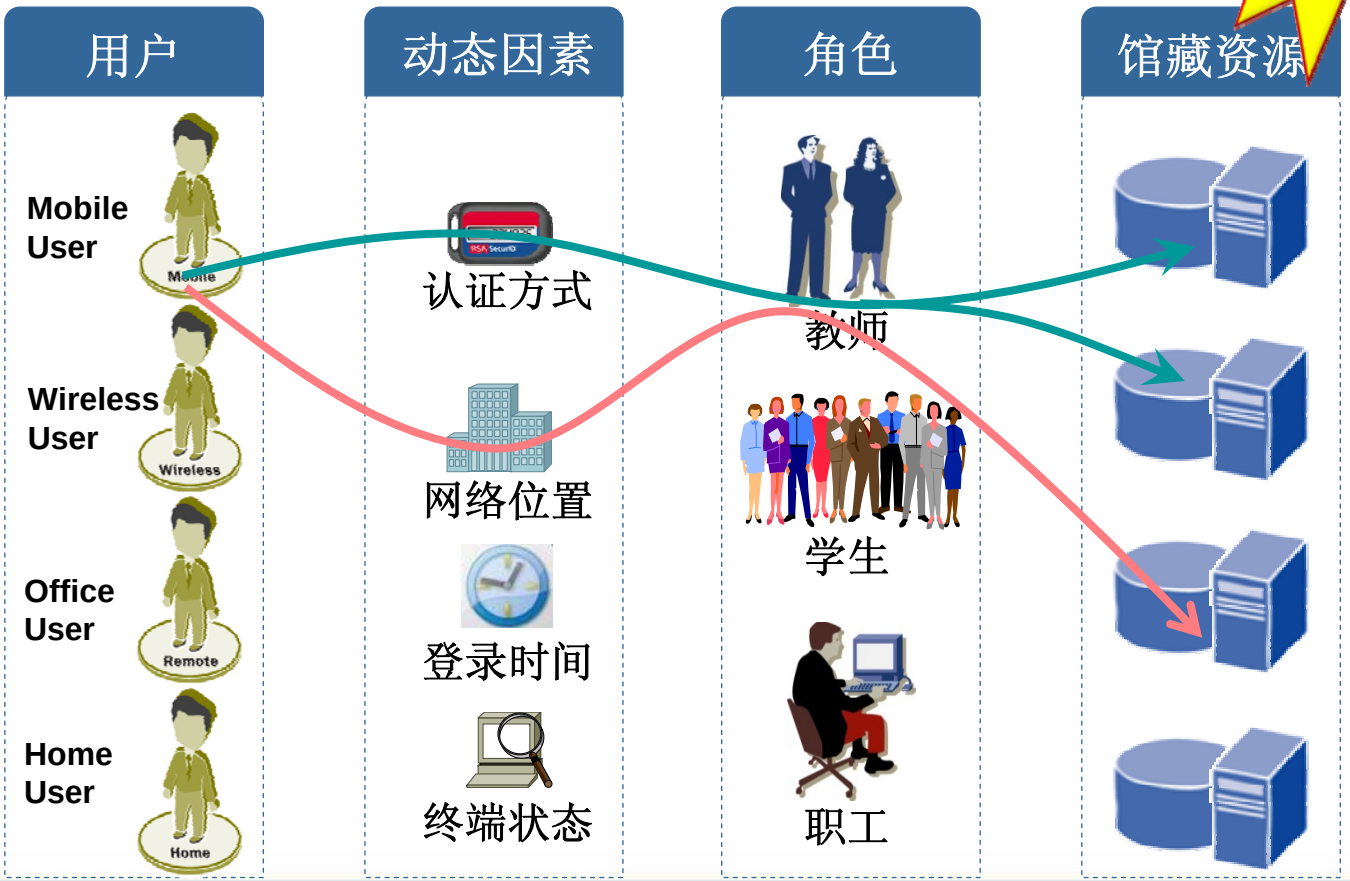


➢统一校园认证：可整合校园现有认证系统；

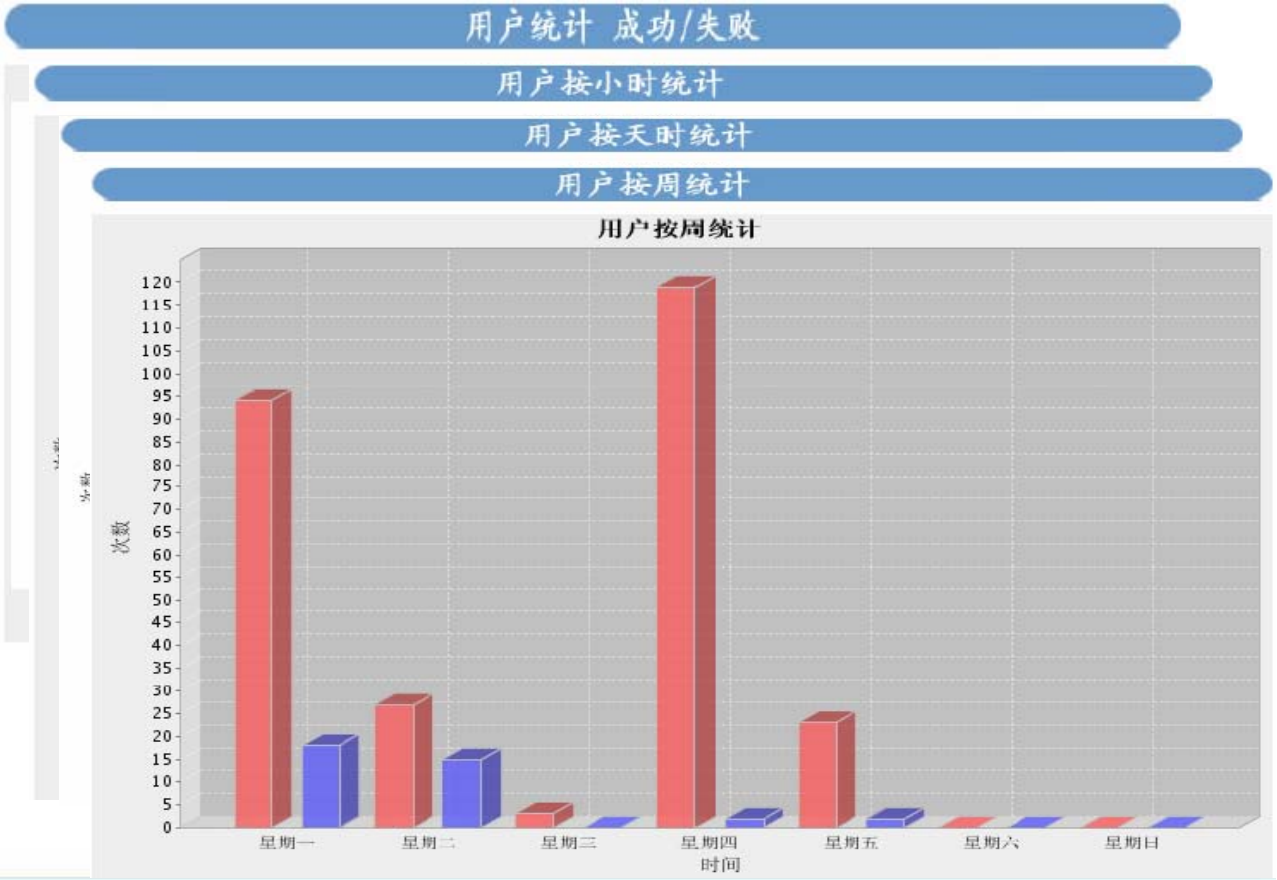
- 免装客户端为用户、管理者带来便利
- 单点登录为用户带来便利

连接？ 认证？ 便利？ 权限？ 审计？

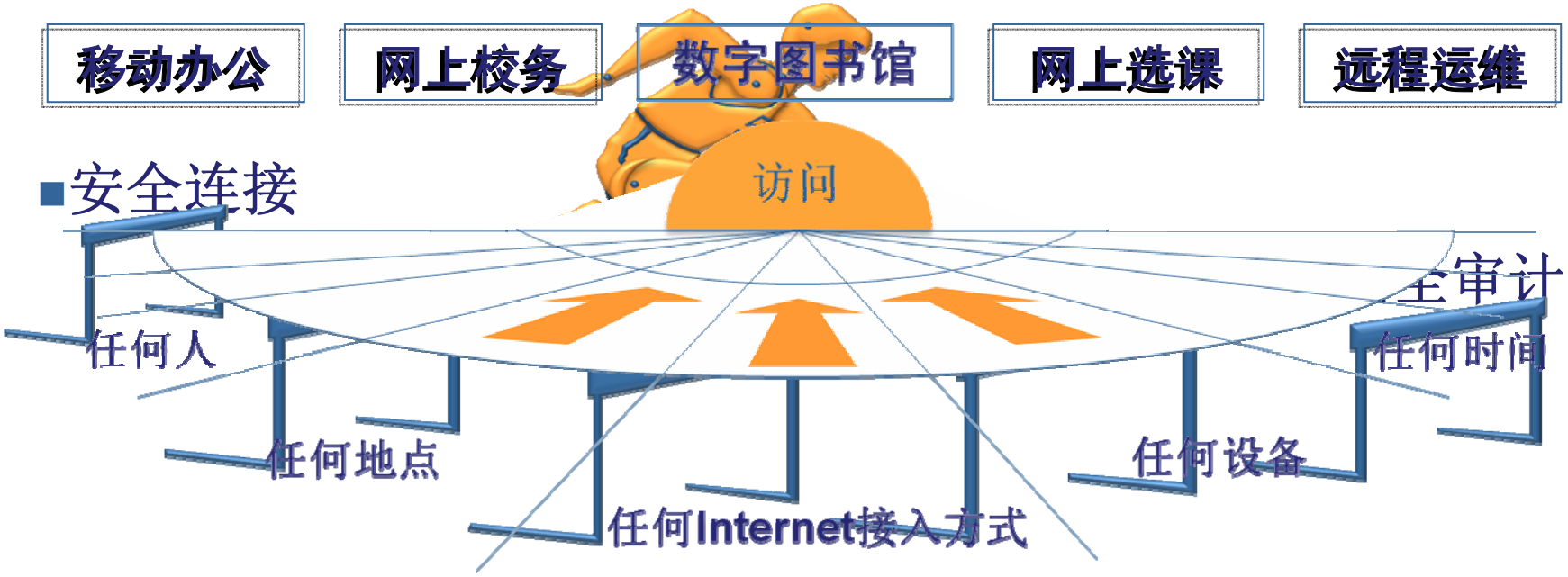

动态权限
管理


用户
动态因素
角色
馆藏资源
Mobile User
Wireless User
Office User
Home User
Mobile
Wireless
Remote
Home
认证方式
网络位置
登录时间
终端状态
教师
学生
职工

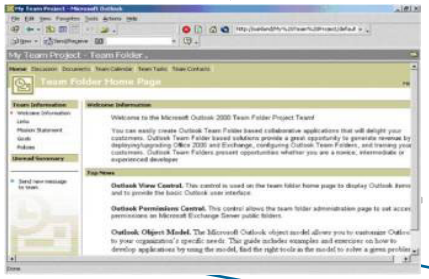
- 详细的审计
  - 用户行为审计
  - 管理员操作审计
  - 系统状态审计
  - 丰富的报表格式
  - 巨大的存储空间



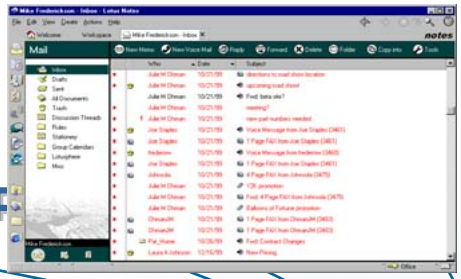
方案小结


移动办公
网上校务
数字图书馆
网上选课
远程运维
访问
■安全连接
任何人
任何地点
任何Internet接入方式
任何设备
任何时间
全审计

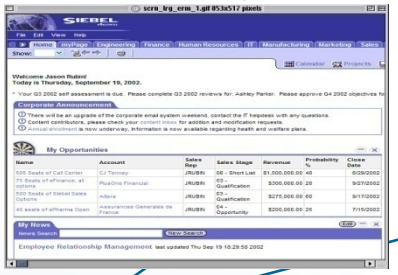
校务管理



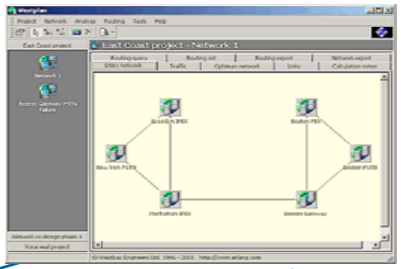
网上选课



数字图书馆



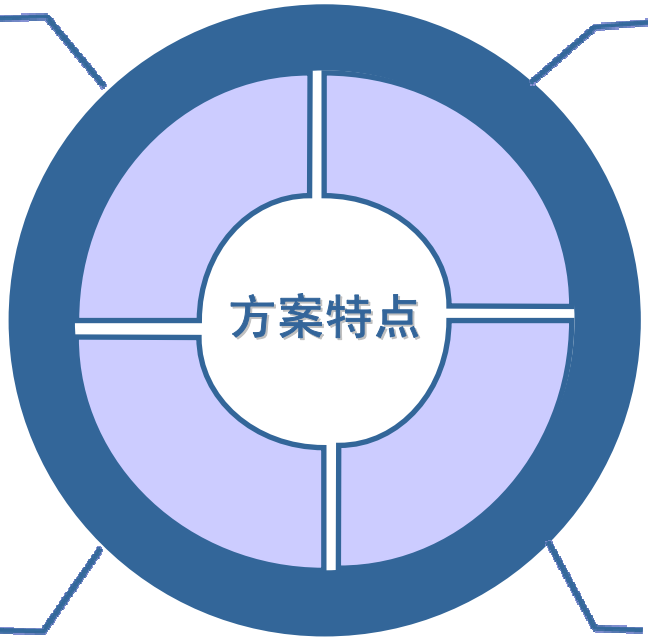
远程运维



认证、控制、权限、审计

校园

方案特点



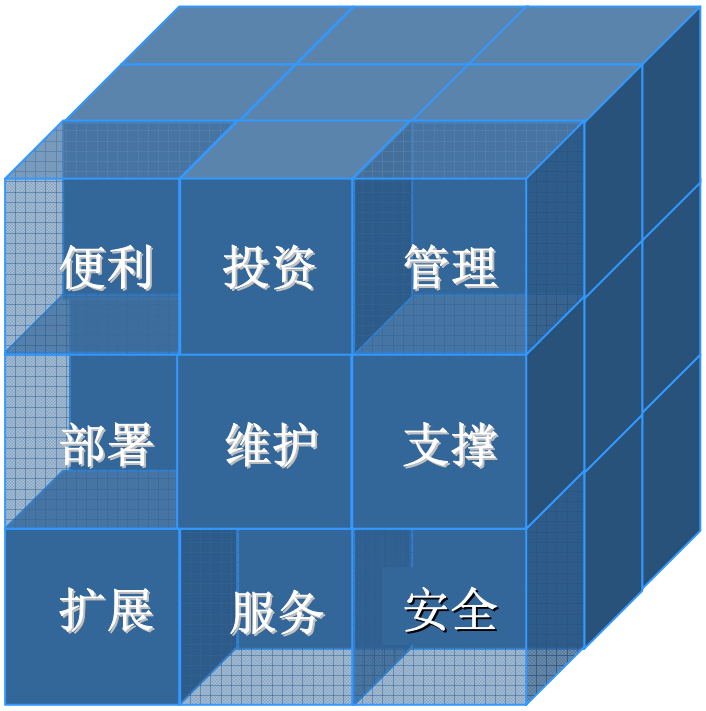
简易性
- 100%零客户端
- 现有授权制度的继承
- 现有用户管理的继承
- 现有的基础设施整合

安全性
- 加密的安全传输
- 细粒度访问控制
- 全面的准入检查
- 详细的安全审计

接入形式多元化
- 任何人
- 任何地点
- 任何设备
- 任何网络接入方式

应用整合
- 数字图书馆
- 网上选课
- 网上校务
- 移动办公

用户价值



- 用户使用便利性
- 降低了设备投资
- 降低了管理成本
- 降低了部署成本
- 维护了原有投资
- 支撑了应用安全
- 保障2-3年可扩展性
- 保障本地化服务

教育行业主推产品

普通学院

普通学院

综合大学

SAG－800

- 加密吞吐200Mbps
- 800个并发用户
- 硬件加速
- 4个10/100/1000Base-T接口
- 串口/短信modem接口
- 1U标准机箱

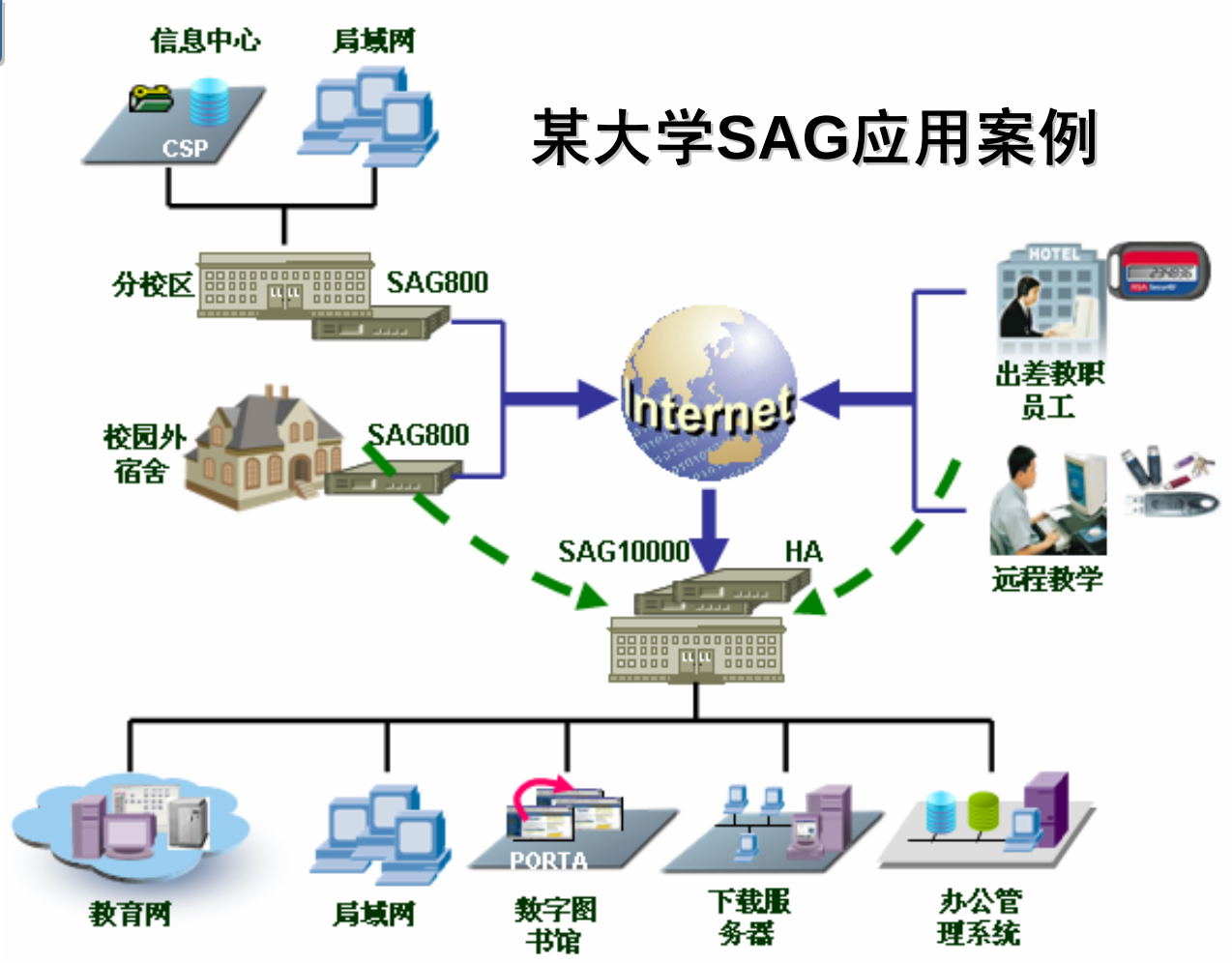
SAG－2000

- 加密吞吐400Mbps
- 2000个并发用户
- 硬件加速
- 4个10/100/1000Base-T接口
- 4个SFP插槽
- 串口/短信modem接口
- 2U标准机箱
- 冗余双电源,热插拔

SAG－10000

- 加密吞吐900Mbps
- 10000个并发用户
- 硬件加速
- 4个10/100/1000Base-T接口
- 4个SFP插槽
- 串口/短信modem接口
- 2U标准机箱
- 冗余双电源,热插拔

应用案例


某大学SAG应用案例
信息中心
局域网
CSP
分校区
SAG800
校园外
宿舍
SAG800
Internet
HOTEL
出差教职
员工
远程教学
SAG10000
HA
教育网
局域网
PORTA
数字图
书馆
下载服
务器
办公管
理系统

成功案例


中国数字图书馆建筑设计分馆
CHINA DIGITAL LIBRARY ARCHITECTURAL DESIGN DIGITAL LIBRARY
欢迎登录中国数字图书馆建筑设计分馆！
附加码：
CSD2
输入名字：
输入口令：
附 加 码：
登录系统
安装可信证书链
修改口令


CDISS
数字信息资源与服务体系
欢迎使用CDISS服务！
输入名字：
输入口令：
自动登录：
登录


重庆大学
CHONGQING UNIVERSITY


北京師範大學
BEIJING NORMAL UNIVERSITY


云南大学


国家自然科学基金委员会
National Natural Science Foundation of China

为数字校园保驾护航！

更多信息，请登录：http://www.leadsec.com.cn
客户热线：010-82427766
免费客服：400－810－7766

联想网御科技（北京）有限公司