



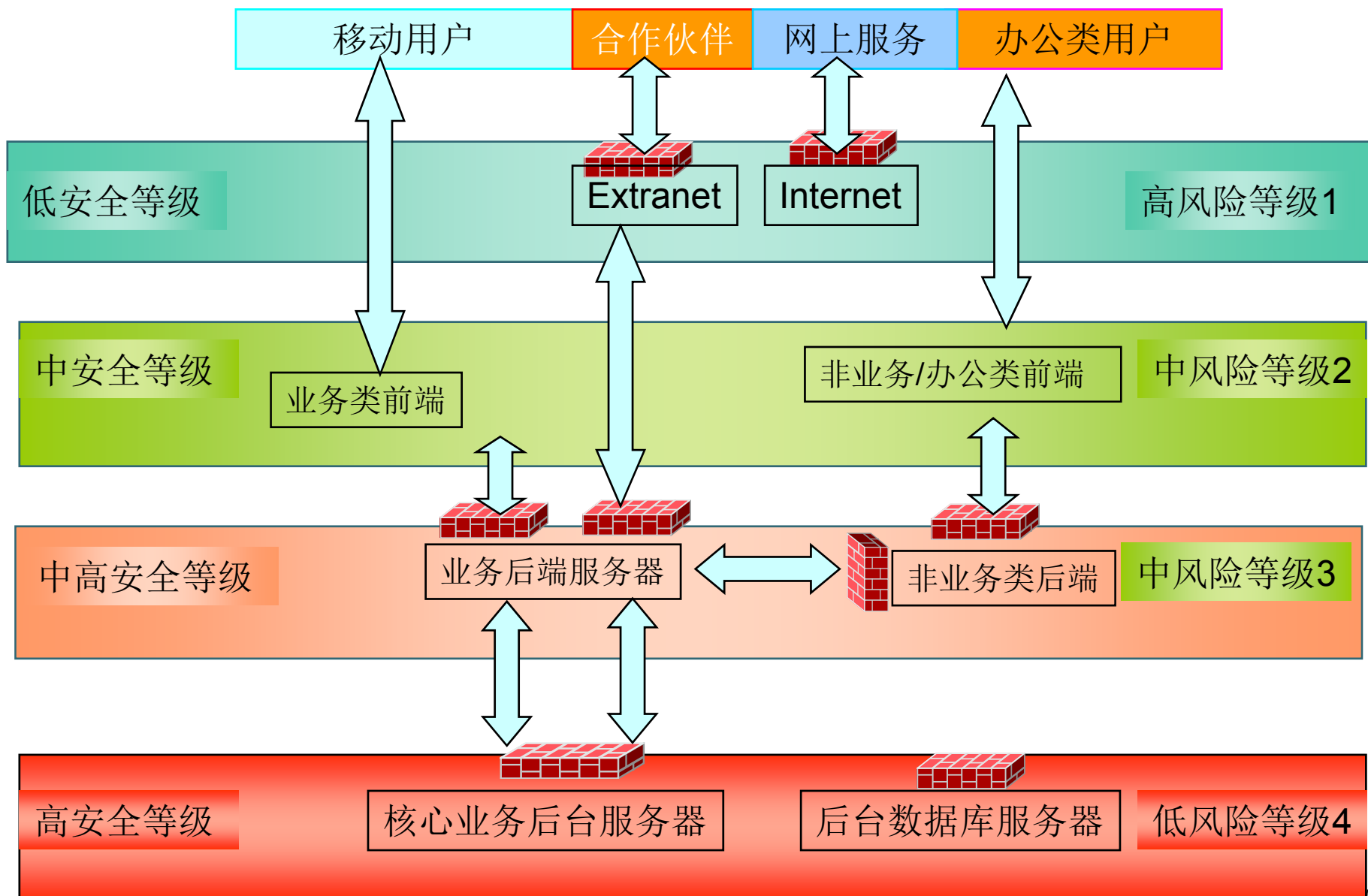
COMBAT-LAB

企业级网络项目实战

企业数据中心设计建议

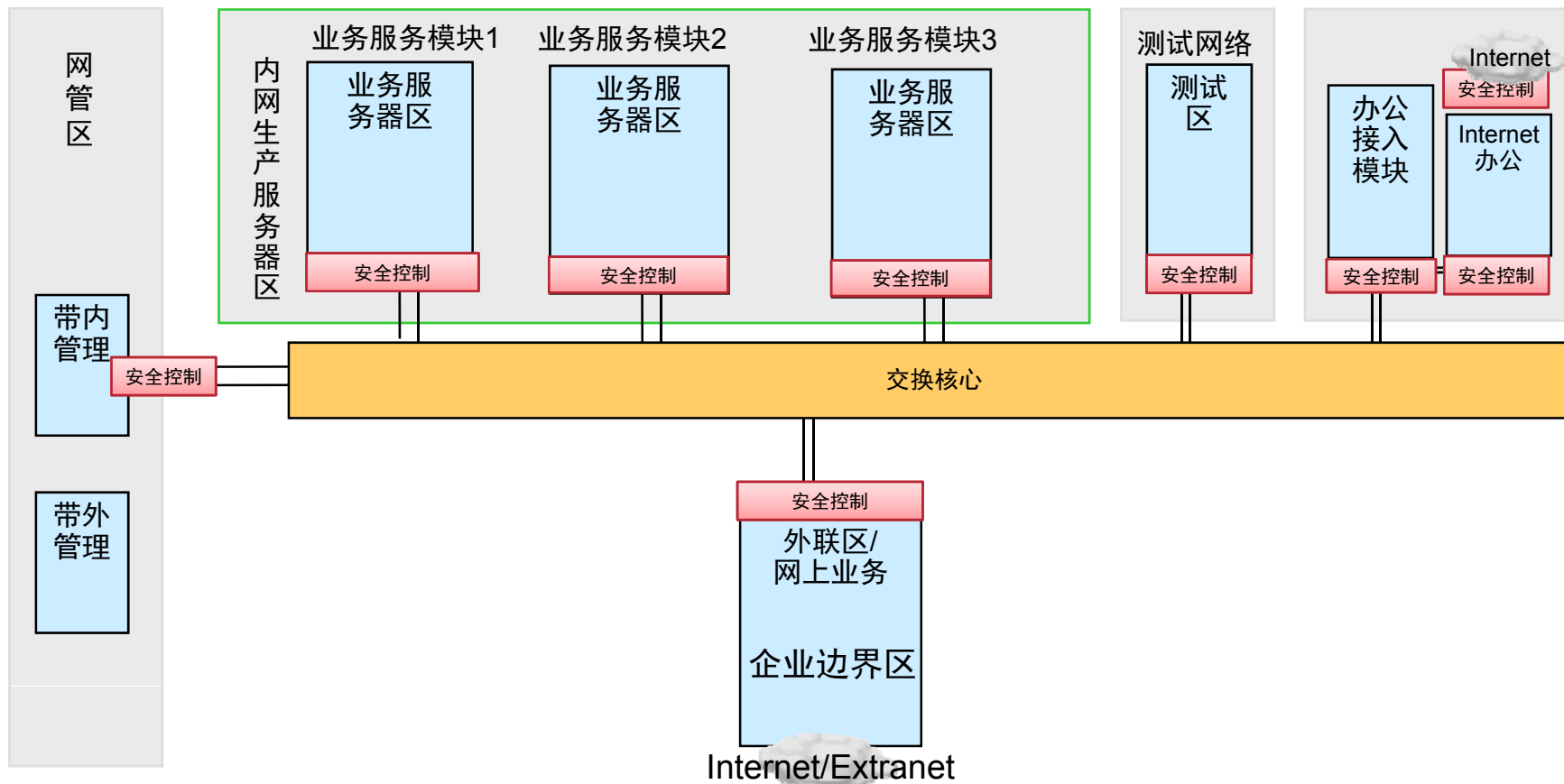


数据中心安全设计模型参考

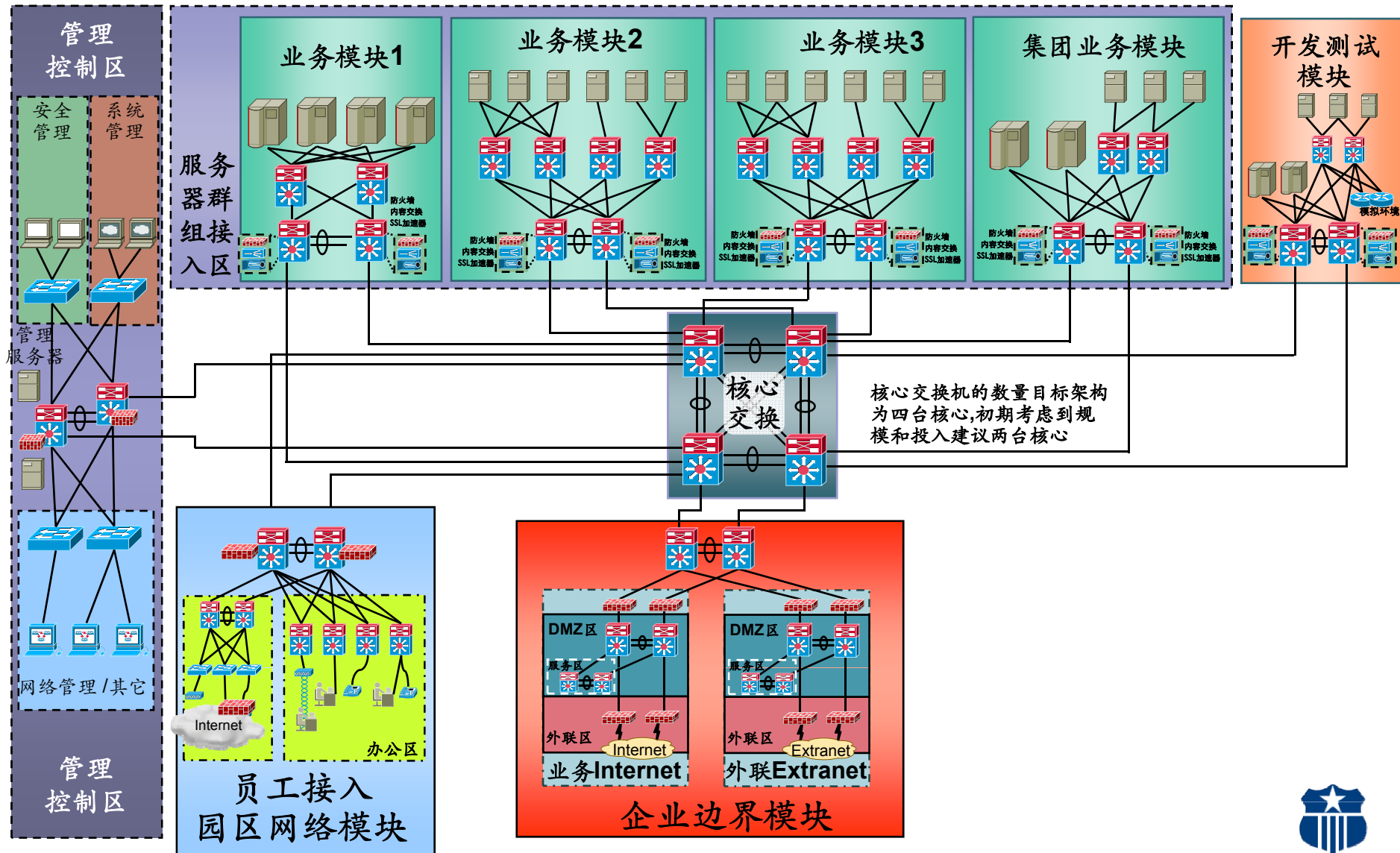


AB

数据中心分区架构示意图



数据中心网络架构示意图

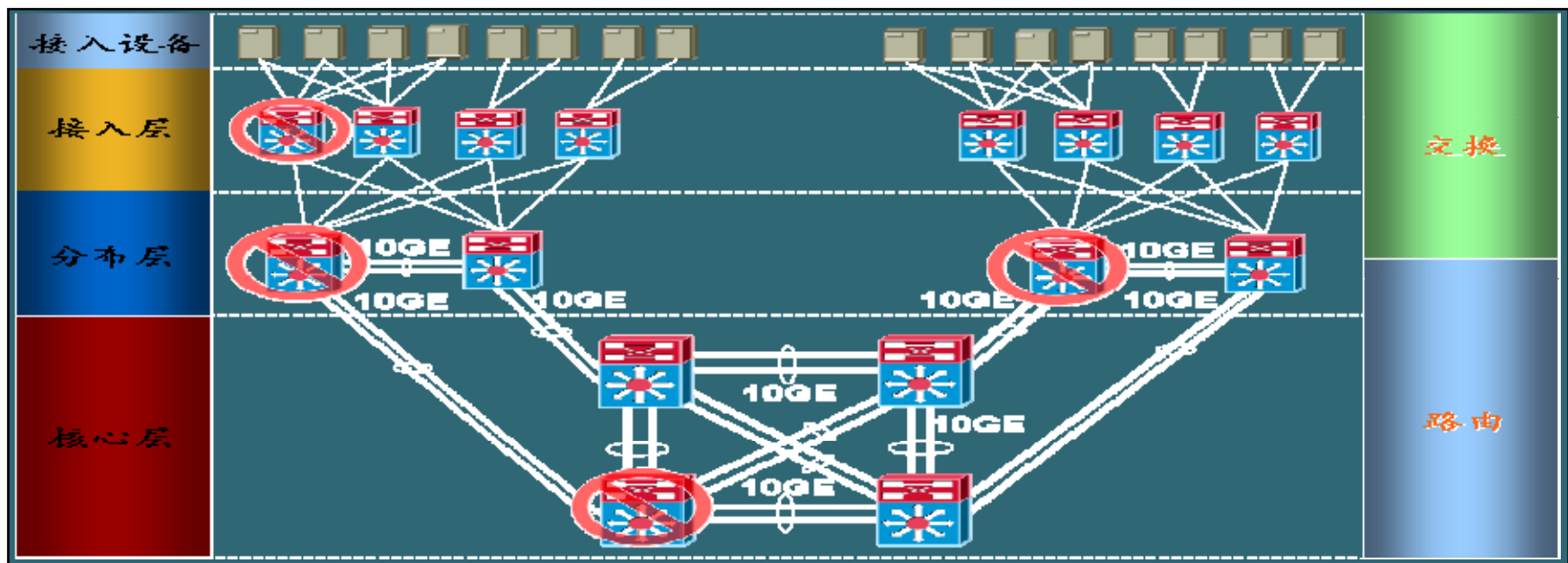


- 交换核心概要设计
- 服务器区域概要设计
- 边界区域设计
- 数据中心员工接入
- 开发测试区设计
- 数据中心存储
- 网络运维管理



数据中心高可用性网络架构建设

层次化网络架构设计



分层部署部署要点：

- 根据应用系统架构，进行网络层次和区域划分
- 模块化分层部署，增强系统弹性
- 核心层与汇聚层通过万兆接口采用3层连接
- 汇聚层与接入层通过万兆或千兆接口采用2层连接（接入层采用L2设计，也可以采用L3）
- 多链路负载均衡设计，避免出现单点/多点故障



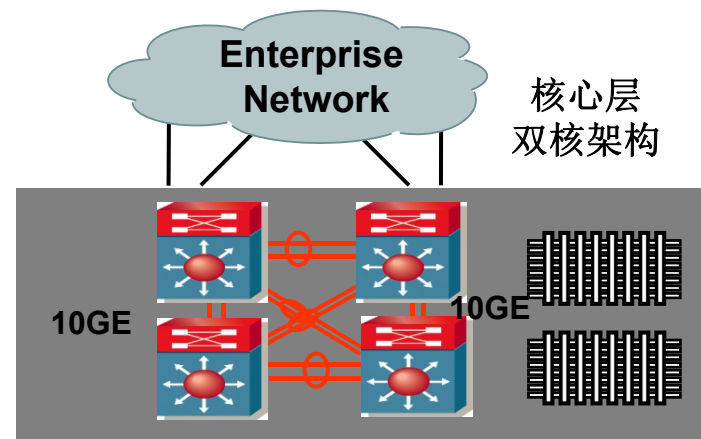
数据中心核心层设计说明

核心层说明:

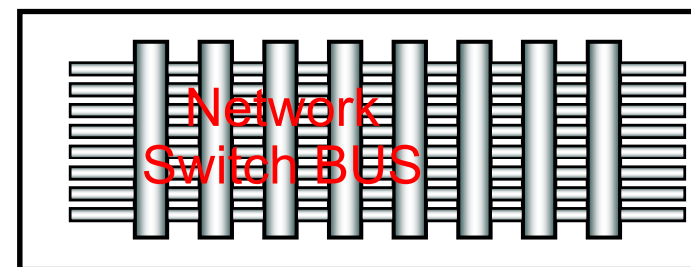
数据中心核心层连接各个功能模块是网络的核心枢纽,连接各个模块的核心枢纽,实现多个模块之间的高速连接和数据的快速转发,是数据中心网络最重要的部分;

核心交换区域特性要求:

- 高性能快速转发;高密度10GE连接
- 高可靠性/可用性
- 超载比尽可能小
- 可扩展性高
- 3层互连但要考虑兼顾DCE技术的发展
- 较高的稳定性
- 满足数据中心数据和存储业务的发展



NSB 网络交换总线 Network Switch Bus



COMBAT-LAB

数据中心核心层设计说明

部署建议

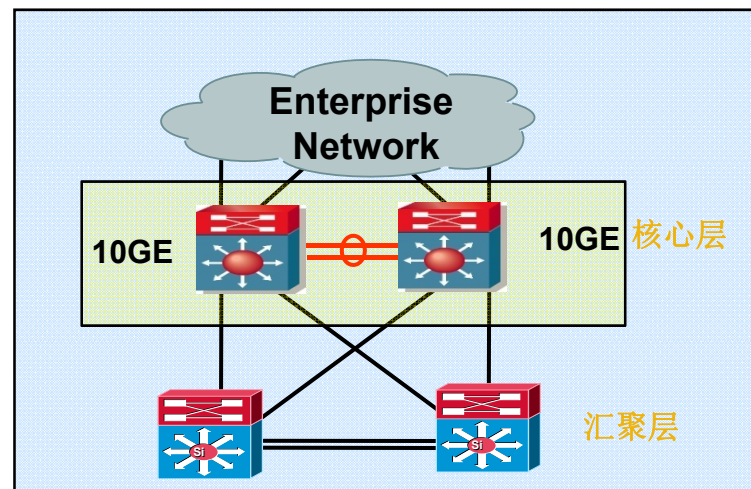
标准设计参考:

- 两台高性能设备为核心交换机,
- 核心设备、设备部件、链路冗余设计
- 核心层与分布层之间采用L3连接
- 支持数据中心高密度10GE能力,有支持下一代数据中心DCE,FCOE等技术的能力
- 适合中等规模企业数据中心
- 初期建议采用这种模式

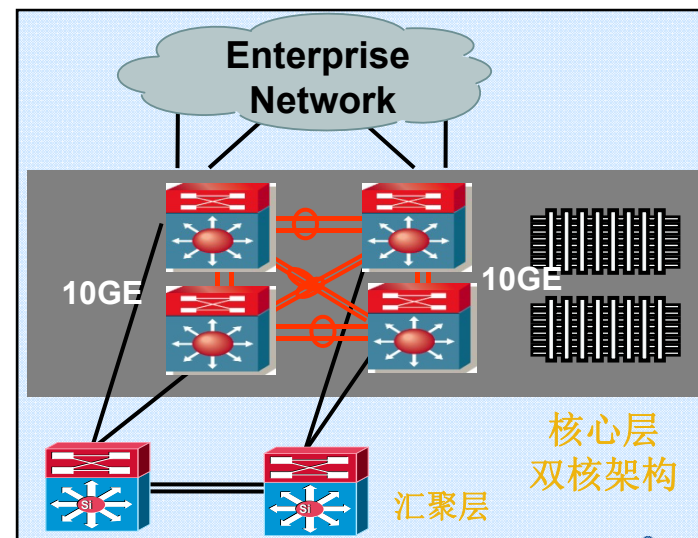
新一代核心层设计参考:

- 四台高性能设备为核心,可以部署为双核心双总线
- 核心设备、设备部件、链路冗余设计
- 支持数据中心高密度10GE能力,有支持下一代数据中心DCE,FCOE等技术的能力
- 核心层与分布层之间采用L3连接
- 核心区内部三角连接,和每个汇聚功能区交换机分别连接到(左右)双核心
- 适合大中规模企业数据中心,对可靠性要求较高的数据中心
- 将来的目标架构

本次架构



目标架构



根据需要可以初期采用通用设计,将来扩展时采用目标架构

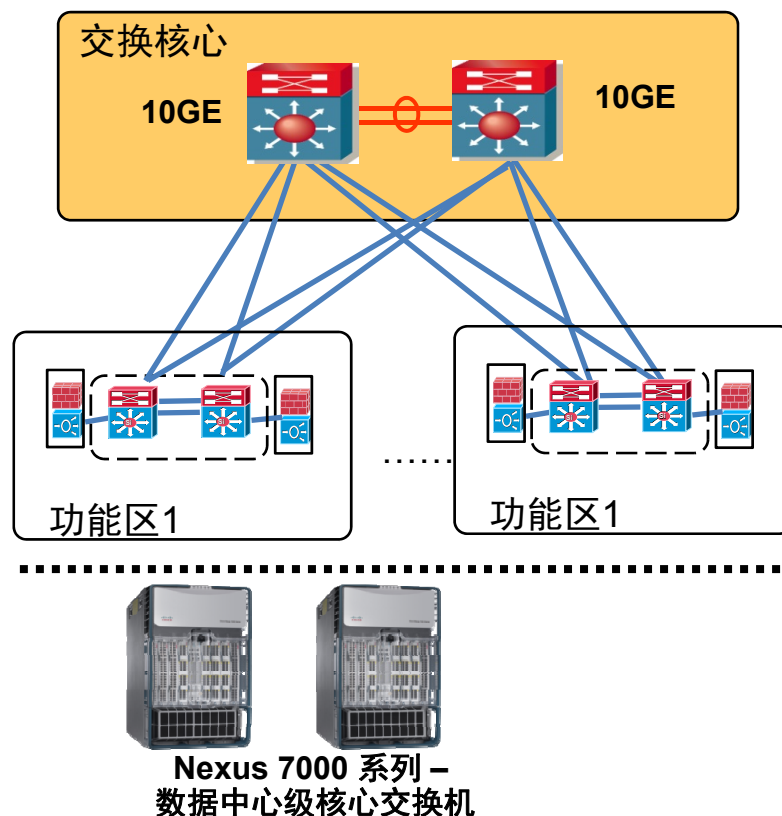
交换核心的参考设计

本次架构设计参考：

- 结构设计：2台设备组建核心、选用最快速收敛的路由协议，2个物理区域部署，跨板卡连接同一区域，安全控制在接入层实现
- 设备选择：选择高可靠设备；引擎、风扇1+1冗余、交换矩阵、电源N+1冗余；支持引擎不间断业务切换、支持不丢包传输和二层多路径技术，需要高密度万兆板卡；建议部署思科数据中心交换机Nexus7000，
- Nexus7000支持DCE数据中心以太网技术，FCoE技术，支持高密度万兆接口，99.999%高可靠性设计；
- 扩展考虑：具体配置端口数量可以业务需求部署相应模块端口
- 运维要求：具备自监控能力、配置可自动回退，基于不同人员的角色权限管理；

可方便的扩展到目标架构：

- 随着业务的扩展和对可靠性的增加，可以方便将现在的两台核心架构扩展到四台为核心的架构，可靠性将大大增加；
- 随着数据中心技术发展：目前的Nexus已经支持I/O整合、FCoE、DCE、虚拟化技术，平滑满足数据中心的整合和发展；
- 即使扩展到四台交换机核心，对各个汇聚功能区没有影响



- 统一交换架构技术' Unified fabric'
- lossless无丢包矩阵结构，面向DCE FCoE
- 高密度万兆接口，面向 40GbE/100GbE
- 业务零中断的设计，99.999%可靠性
- 不间断的系统操作
- 目前4.1T交换能力 可达15Tb+ 交换能力



COMBAT-LAB

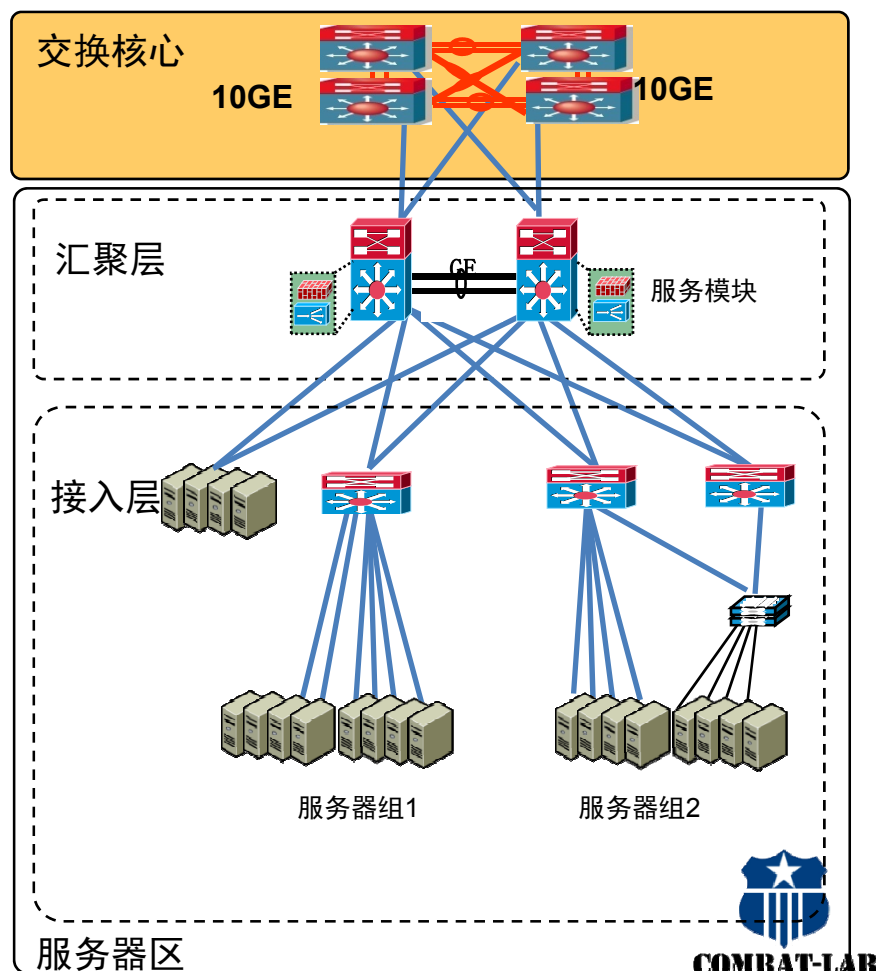
- 交换核心设计
- 服务器区域设计
- 边界区域设计
- 数据中心员工接入
- 开发测试区设计
- 数据中心存储
- 网络运维管理



业务服务器区设计需要考虑的问题

业务服务器区是公司提供服务的业务服务器区。因此需要考虑较高的可用性和更全面的安全防护措施。按照层次化模块化的设计理念，服务器区的网络可分为汇聚层和接入层两层，功能定位和设计思路各不相同。

- **汇聚层：承上启下，连接核心层和接入层，为区域内的服务器提供网络服务，主要的设计思路包括：**
 - 采用服务模块的方式，提供防火墙，负载均衡，及SSL卸载等网络服务
 - 访问业务服务区需要通过防火墙控制，业务区之间访问需要通过防火墙策略控制，具体的策略控制更具各个业务区要求而定
- **接入层：汇接服务器，上联到汇聚层。为了解决可用性和扩展性需求和可管理性需求，主要的设计思路包括：**
 - 服务器的高性能接入，可采用TOR和EOR等组和设计。
 - 尽可能消除二层环路，提高可用性
 - 高扩展性的服务器群，采用模块化交换机解决服务器物理布局扩展性问题
 - 采用网络设备虚拟化和服务器虚拟化，提高可扩展性
 - 考虑将来存储和IP网融合和统一I/O技术



数据中心服务器区流量的超载比设计

服务器区满足容量需求的主要方式是进行超载比设计。超载比是指网络设备downlink和uplink的带宽比例

接入层超载比计算考虑的因素

- 服务器内部总线类型
- 服务器CPU数量, CPU核数量, 网卡数量
- 服务器接口是否双活
- 服务器磁盘I/O方式和应用类型

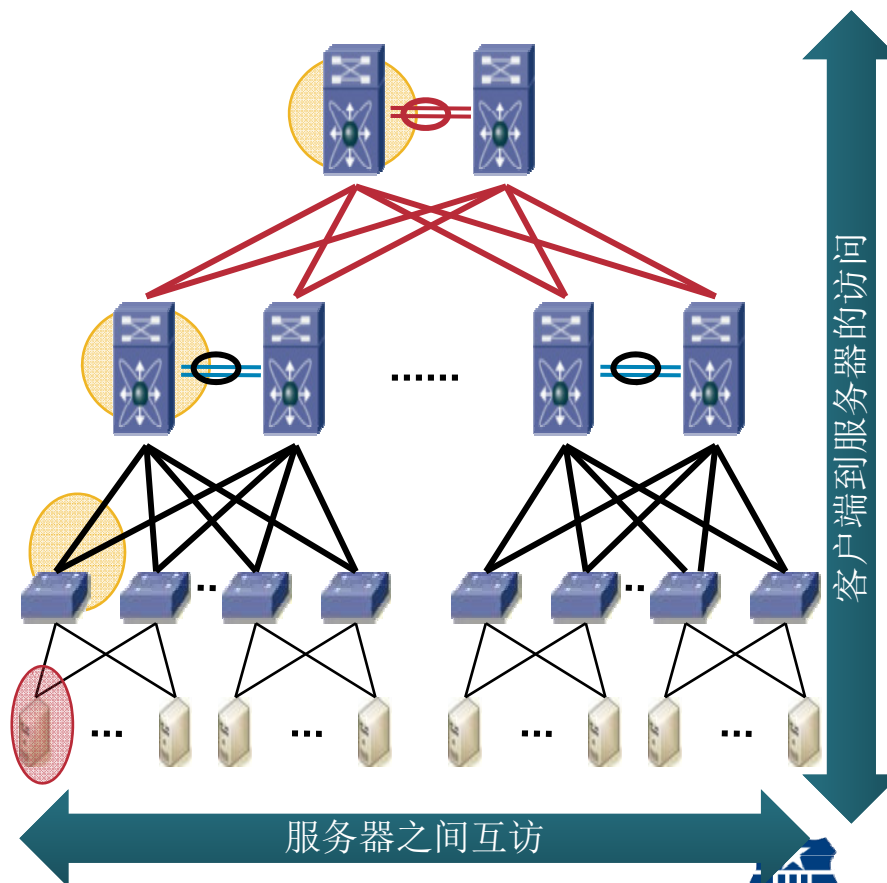
汇聚层超载比计算考虑的因素

- 系统架构
- 板卡类型
- Uplink /downlink比例

典型比例: 4:1 up to 12:1

推荐超载比

连接的服务器类型	推荐建议
Web服务器	12:1
App服务器	6:1
DB服务器	4:1



COMBAT-LAB

特性要求： 高可靠性、高安全性、高扩展性、实现业务的分类和业务的接入和流量控制。

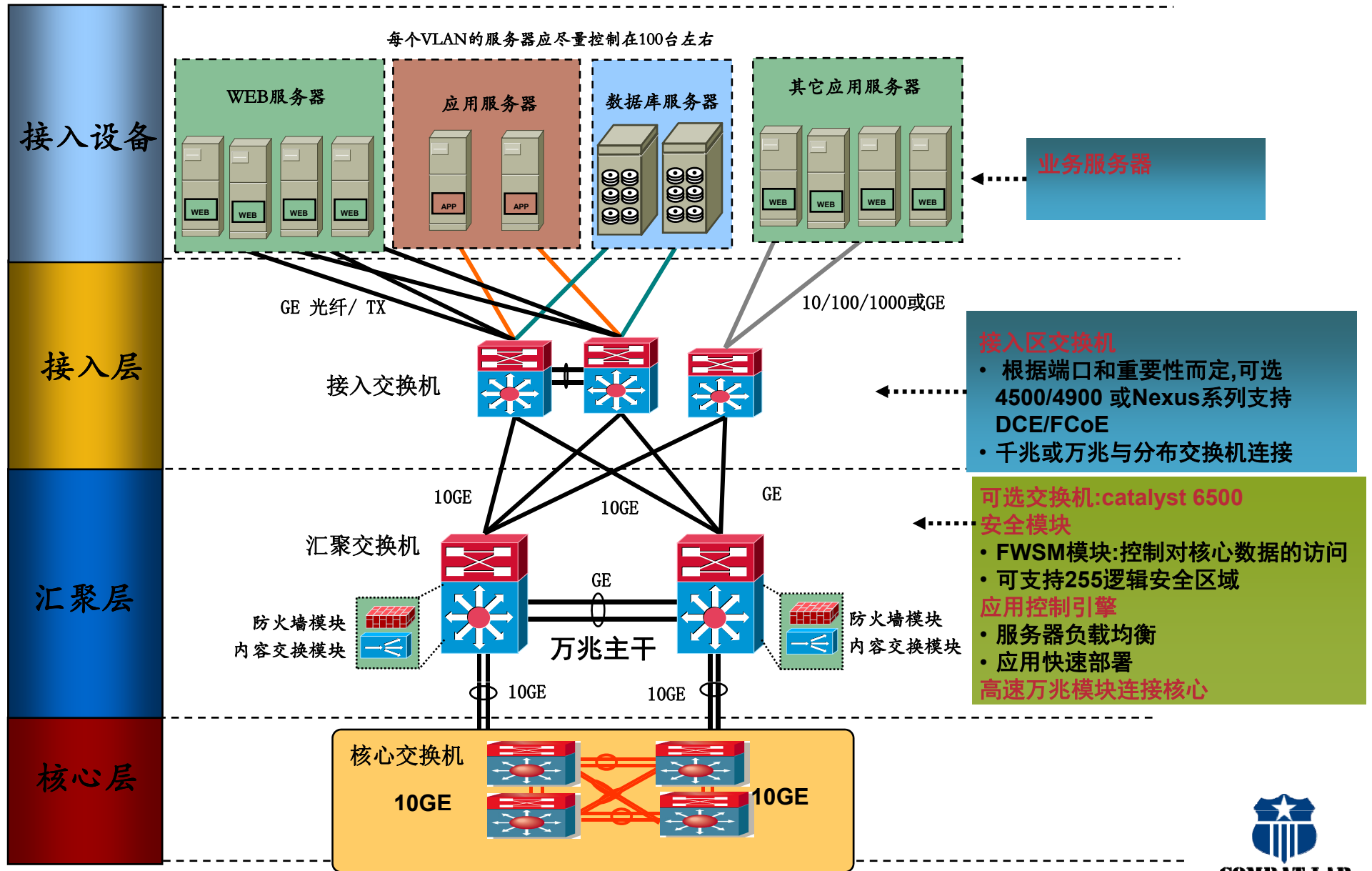
设备部署建议：

- 汇聚层建议部署：部署思科catalyst 6500 VSS交换机, 部署内置防火墙模块和L4-L7应用负载
- 接入层部署：根据服务器的多少, 可以部署Cat4500/Cat4900（具体设备和端口根据需要选择）
- 汇聚到核心层采用万兆连接, 汇聚到接入层采用千兆连接, 利用VSS做到负载均衡



COMBAT-LAB

业务服务器区网络模块设计- 模式一



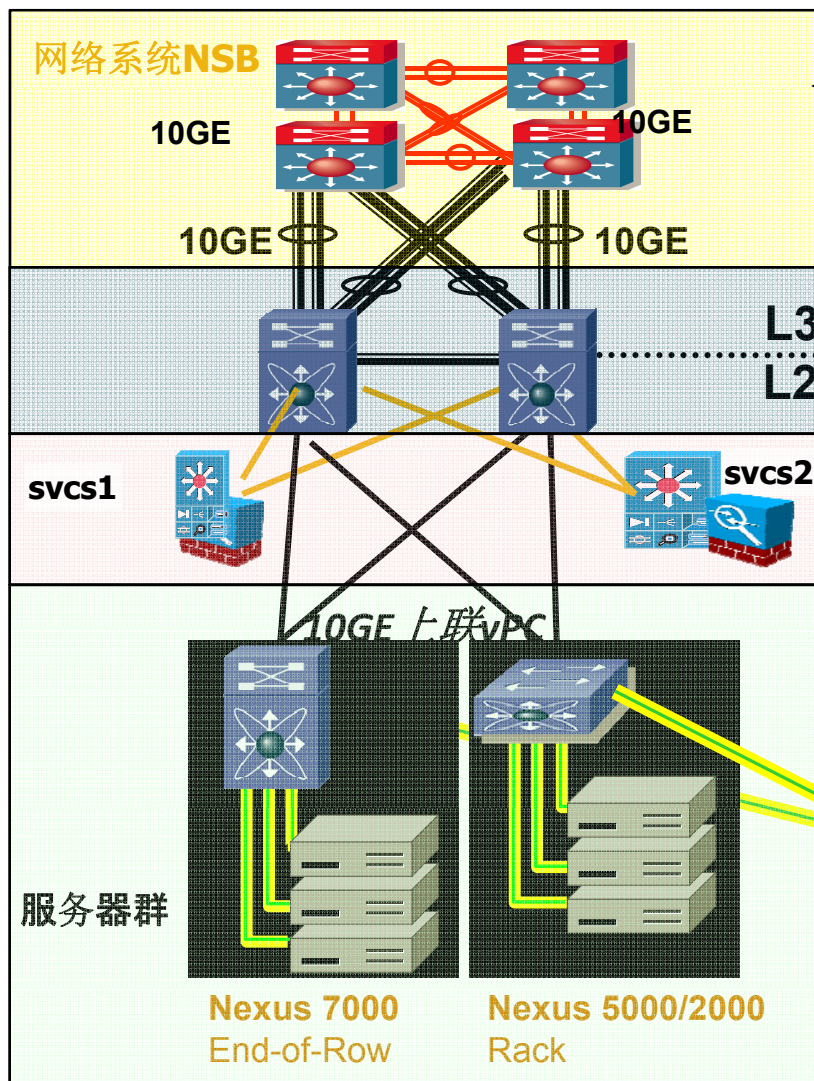
业务服务器区网络模块设计-模式二

考虑到数据网络和存储的整合

核心层
高性能万兆核心

汇聚层
1 高性能万兆和千兆模块
2 网络安全和应用服务区

接入层
支持高密度GE
支持TOR/EOR灵活部署
支持数据中心技术FCOE的融合



核心数据区交换机

- 参考配置 :Nexus7000
- 万兆交换模块:与分布交换机连接

核心数据区交换机

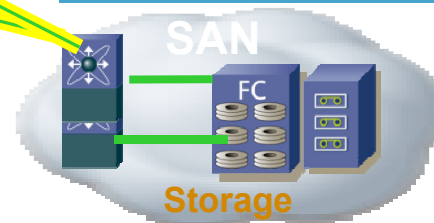
- 参考配置: Nexus7000
- 高密度万兆和千兆交换模块

安全模块:参考配置

- Cat6500/FWSM模块/部署
- ASA5580高性能防火墙
- 应用控制引擎
- 高速万兆模块连接核心和接入层

接入区交换机

- 在接入层部署参考配置
- N5K/7K或N5K/N2K



存储系统



- 交换核心设计
- 服务器区域设计
- 边界区域设计
- 数据中心员工接入
- 开发测试区设计
- 数据中心存储
- 网络运维管理



边界网络区设计说明:是企业内部对外 **Extranet** 连接(外联业务和Internet业务)的重要区域, 外联网络区域主要包括:

- **外联业务:**实现同其第三方单位业务互通, 通过**Extranet**访问其它单位和业务处理
 - 最终用户、工程公司等外联
 - 兼顾多种外联方式: 由于外联单位比较多,而且每个外联单位的管理要求不完全相同,需要具有灵活性。
- **Internet业务:**为出差, **home office**提供业务及办公服务; 门户网站等。 .

企业边界网络区设计特性要求:

- 风险较大,安全性要求高, 高安全性,高可靠性 ,可扩展性, 可管理性、**DNS**站点技术
- 考略到外联系统的特殊性,能整合的尽量整合, 提高资源利用率
- 企业边界区域的安全性, 建议在该区域配置两重防火墙, 入侵防御系统, 如果可能还需要部署防**DDOS**攻击系统和防病毒网关以及流量监控管理

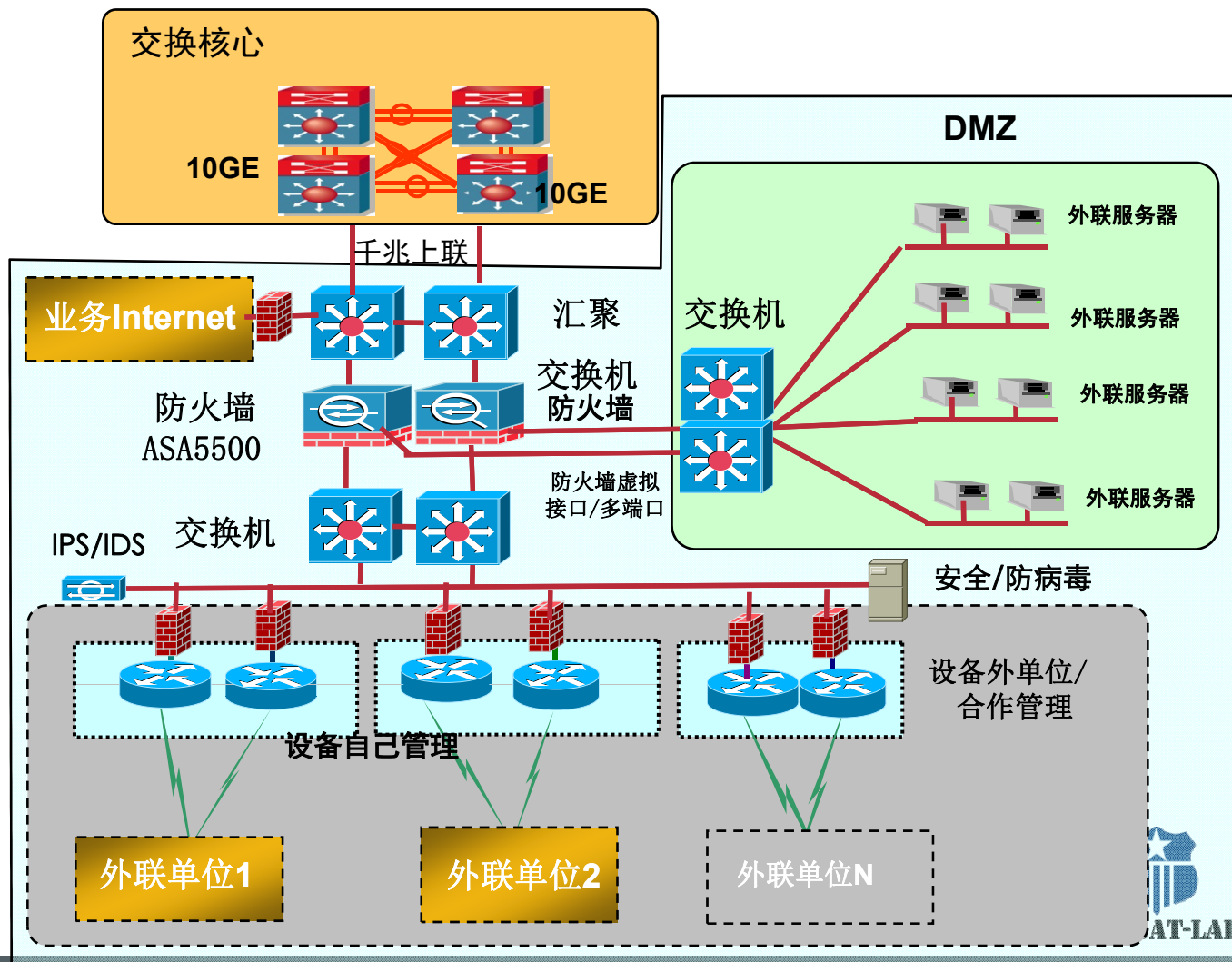


数据中心边界网络区设计说明

外联区Extranet 详细设计示意图

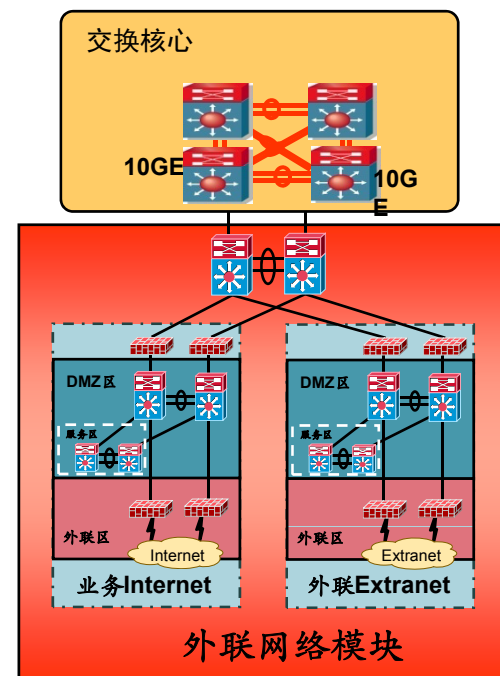
核心交换区域

外联Extranet区域



外联业务区设备部署建议:

- 部署两台接入交换机**cat3750**:考略到外联系统的特殊性,按照外联单位对线路,路由设备和安全的要求,外联单位的隔离需要安全保障,在保持外联单位基本要求的情况下,将各个外联系统接入到接入交换机**cat3750**,考虑到整合和安全要求,需要在交换机**cat3750**分配一个单独的**VLAN**给每个外联业务系统;
- 部署两台接入**ASA5500**防火墙,并配置虚拟端口功能:接入交换机与**ASA5500**防火墙配置**IDS**模块通过虚拟端口连接,相当于每个外联系统连接到防火墙一样,在**ASA5500**防火墙部署**DMZ**区,将外联服务器连接到**DMZ**区,**DMZ**需要两台交换机**cat3750**
- 边界网络区的汇聚交换机**Cat3750/4500**: **ASA5500**防火墙连接到汇聚交换机, **Internet**业务也需要连接到汇聚交换机,汇聚交换机通过高速连接到数据中心核心交换机
- 外联单位对线路,路由设备和安全的设备的基本要求跟据需求部署:
- 建议采用“云防火墙”



COMBAT-LAB

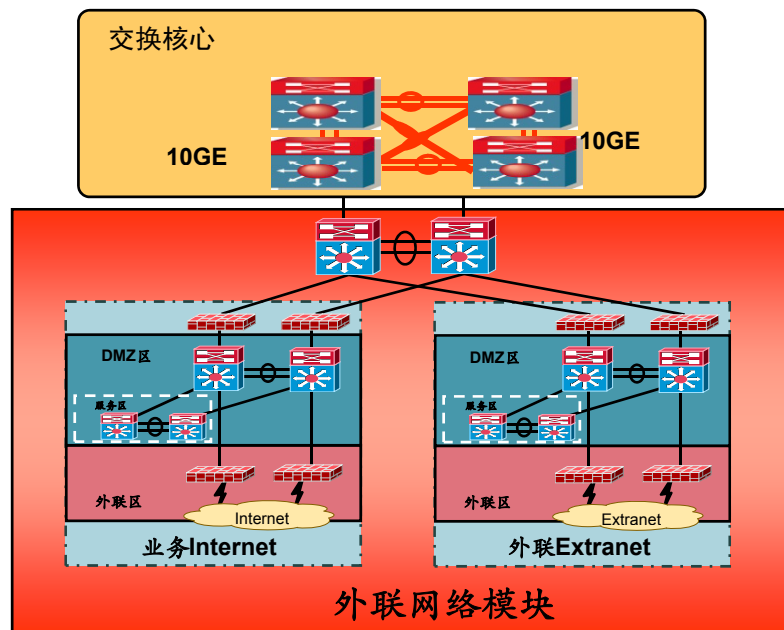
Internet业务:

Internet业务:

- 为出差, home office提供业务及办公服务, 用户通过Internet来访问此区域, 风险相对最大, 对安全性保障要求高.

业务Internet参考建议:

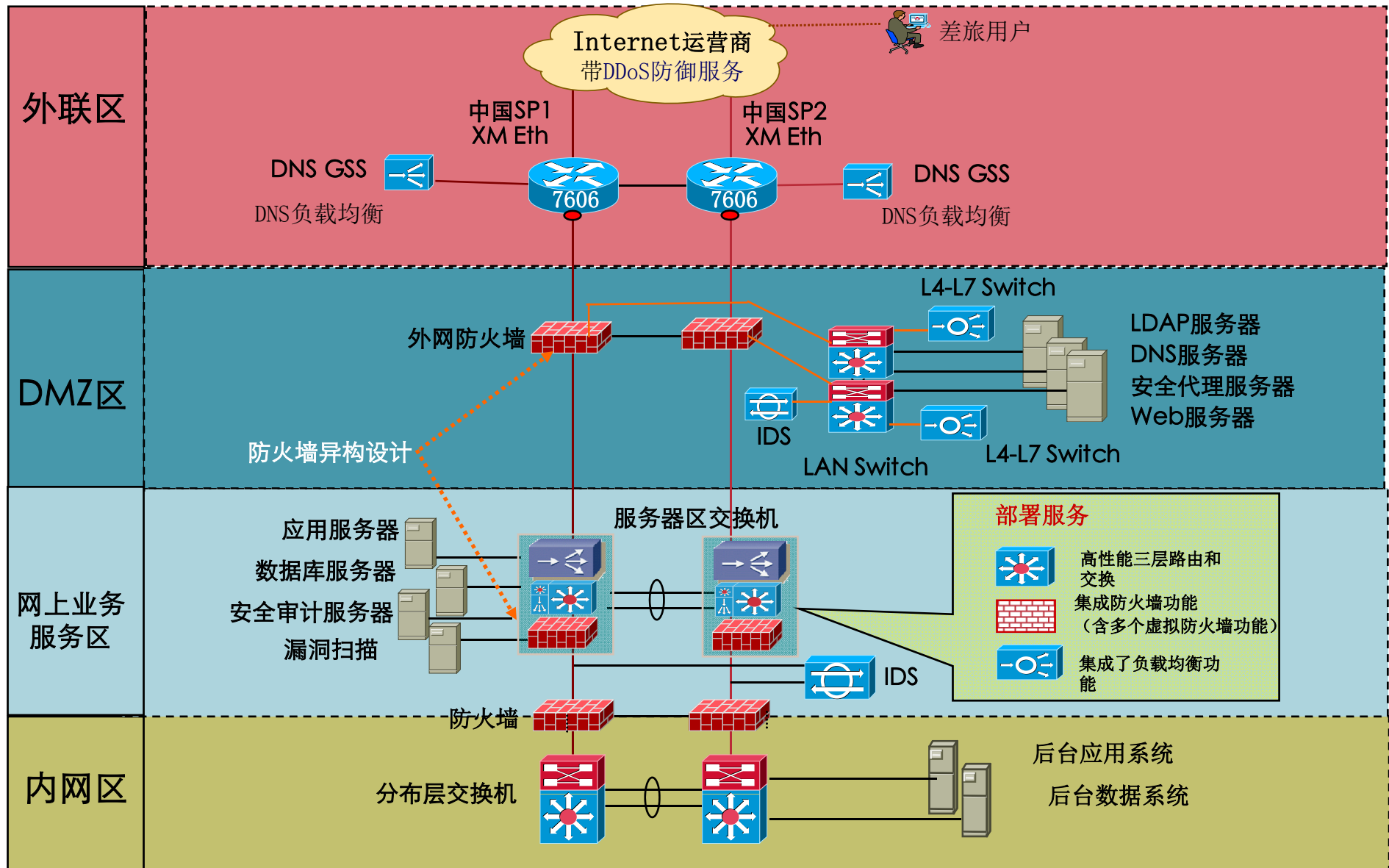
- 采用多层安全层面
- 建议采用“云防火墙”



COMBAT-LAB

数据中心边界网络区设计说明

业务Internet设计 - 参考架构



- 交换核心设计
- 服务器区域设计
- 企业边界区域设计
- 数据中心员工接入
- 开发测试区设计
- 数据中心存储
- 网络运维管理



员工接入网络设计说明:满足数据中心内部员工的接入和管理需求,需要严格的安全控制和管理,

- 企业内部员工访问内部系统:目前**100+**信息点接入需求
- 非本企业员工不允许通过此区域接入内部系统

设计特性要求:

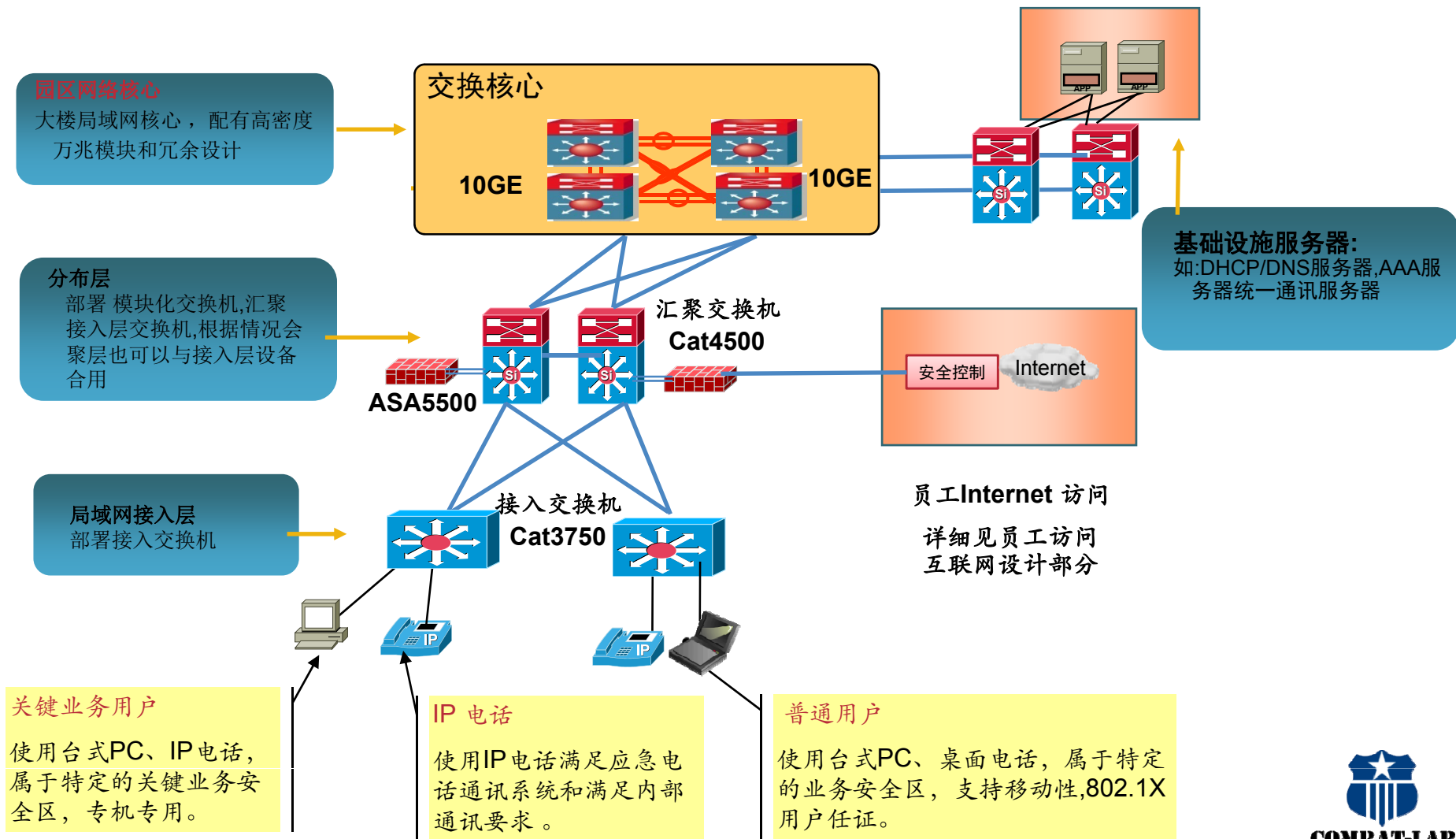
- 安全性管理较高,员工访问的识别和分类,可管理性,高可靠性、可扩展性、**QoS**

设备部署建议:

- 员工接入区按照标准局域网接入设计,可以分为汇聚和接入层,在汇聚层需要考虑安全访问控制,接入层防范非法**PC**接入等;
- 参考建议:汇聚层部署**Cat4500**交换机,配置两台**ASA5500**做安全控制,控制访问数据中心核心网络的安全
- 参考建议:接入层部署**cat3750/3560**交换机,具体配置根据端口数量要求可以灵活选择
- 为了保障接入安全建议部署接入安全控制,如基于**802.1x**身份控制系统,中心部署**AAA**服务器
- 为了实现应急通讯,我们建议部署基于**IP**的应急电话通讯系统



数据中心员工接入网络模块设计



- 交换核心设计
- 服务器区域设计
- 广域网区设计
- 边界区域设计
- 数据中心员工接入
- 开发测试区设计
- 数据中心存储
- 网络运维管理



开发测试网络模块设计说明: 满足数据中心内部员工的开发测试的需求, 同时还需要预留对合作伙伴的开发测试访问端口, 但需要严格的安全控制和管理,

- 企业内部员工开发测试访问接入需求
- 非本企业员工(合作单位)有条件接入终端系统, 只能访问测试区域, 外部人员不能访问人保内部业务系统, 要有严格的监督和安全控制以及管理流程

网络设计特性要求:

- 安全性管理较高, 员工访问的识别和分类, 可管理性, 高可靠性、可扩展性、QoS

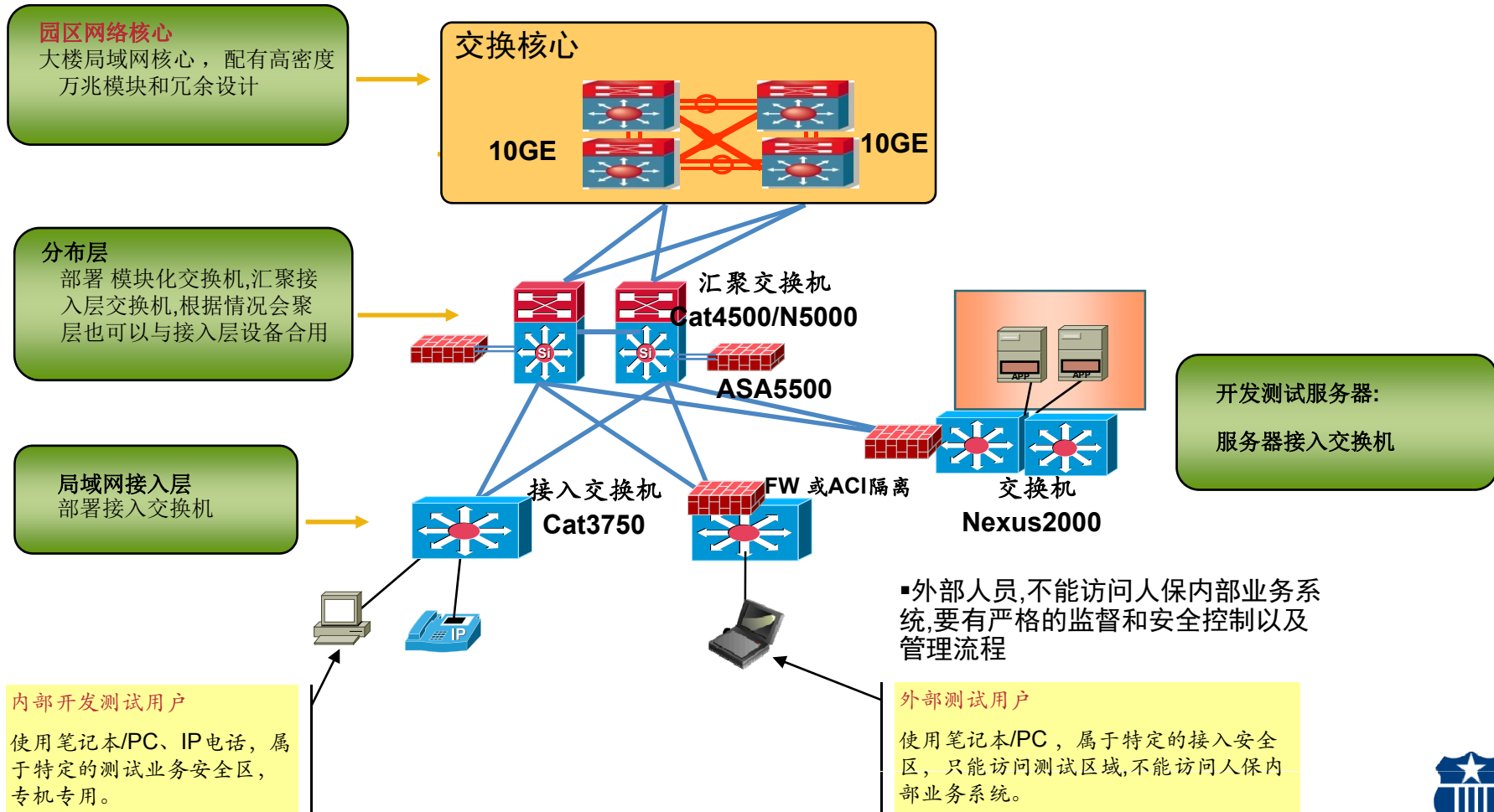
设备部署建议:

- 满足开发测试的要求, 在安全允许范围内, 外部人员有条件接入, 不能访问人保内部业务系统, 要有严格的监督和安全控制以及管理流程
- 为了满足数据中心未来发展, 对先进技术的使用和测试
- 部署参考建议: 汇聚层部署Nexus5000/Cat4500交换机, 配置两台ASA5500做安全控制, 控制访问数据中心核心网络的安全
- 部署参考建议: 接入层部署Nexus2000/cat3750 交换机, 具体配置根据端口数量要求可以灵活选择
- 为了保障接入安全建议部署接入安全控制, 严格端口控制和防火墙策略, 也可以部署基于802.1x身份控制系统



COMBAT-LAB

数据中心开发测试网络模块设计



- 交换核心设计
- 服务器区域设计
- 广域网区设计
- 企业边界区域设计
- 数据中心员工接入
- 开发测试区设计
- 数据中心存储**
- 网络运维管理



数据中心存储网络设计的目标

- 统一规划, 实现存储资源共享
- 存储网络由集团统一管理、建设和维护
- 满足业务的不断扩展的要求

特性要求： 资源共享、实现业务的连续性、统一管理、扩展性

设计内容参考：

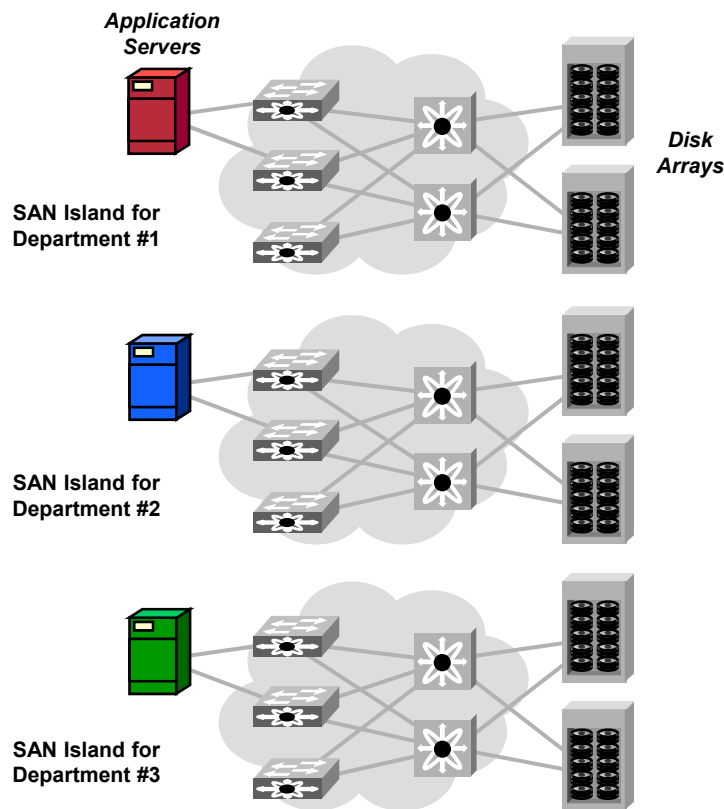
- 存储网络设计
- 通过存储虚拟化技术实现资源整合



存储网络的发展

利用存储虚拟化实现存储网络的优化

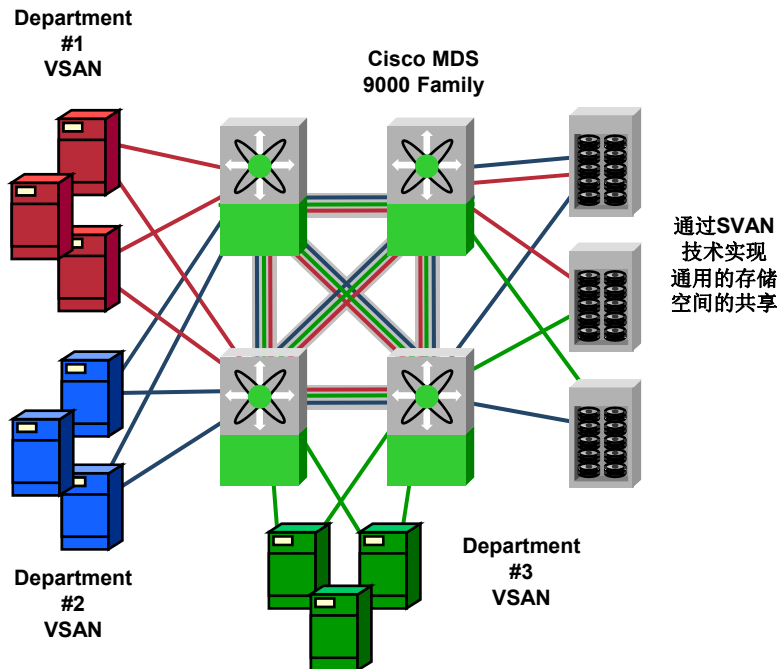
基于应用/部门的存储“孤岛”



独立的物理阵列

每个存储孤岛的预留扩展端口无法利用

数量众多的交换设备需要管理



使用存储虚拟化VSAN 技术 整合的 存储阵列

通用的冗余物理基础架构

无须过多的预留扩展端口 -降低了投资成本 \$\$

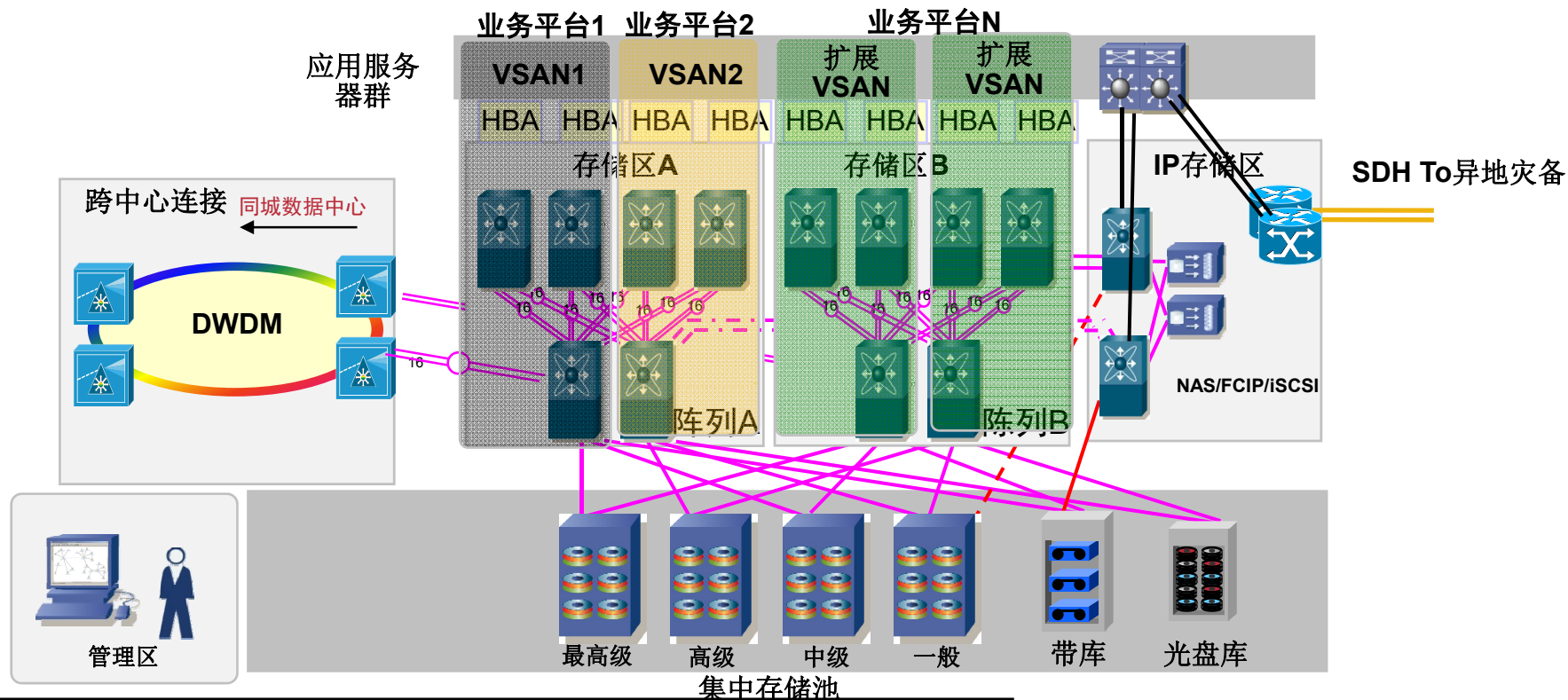
更少的交换设备需要管理

无中断的分配预留的端口



COMBAT-LAB

数据中心存储架构设计规划-远期规划

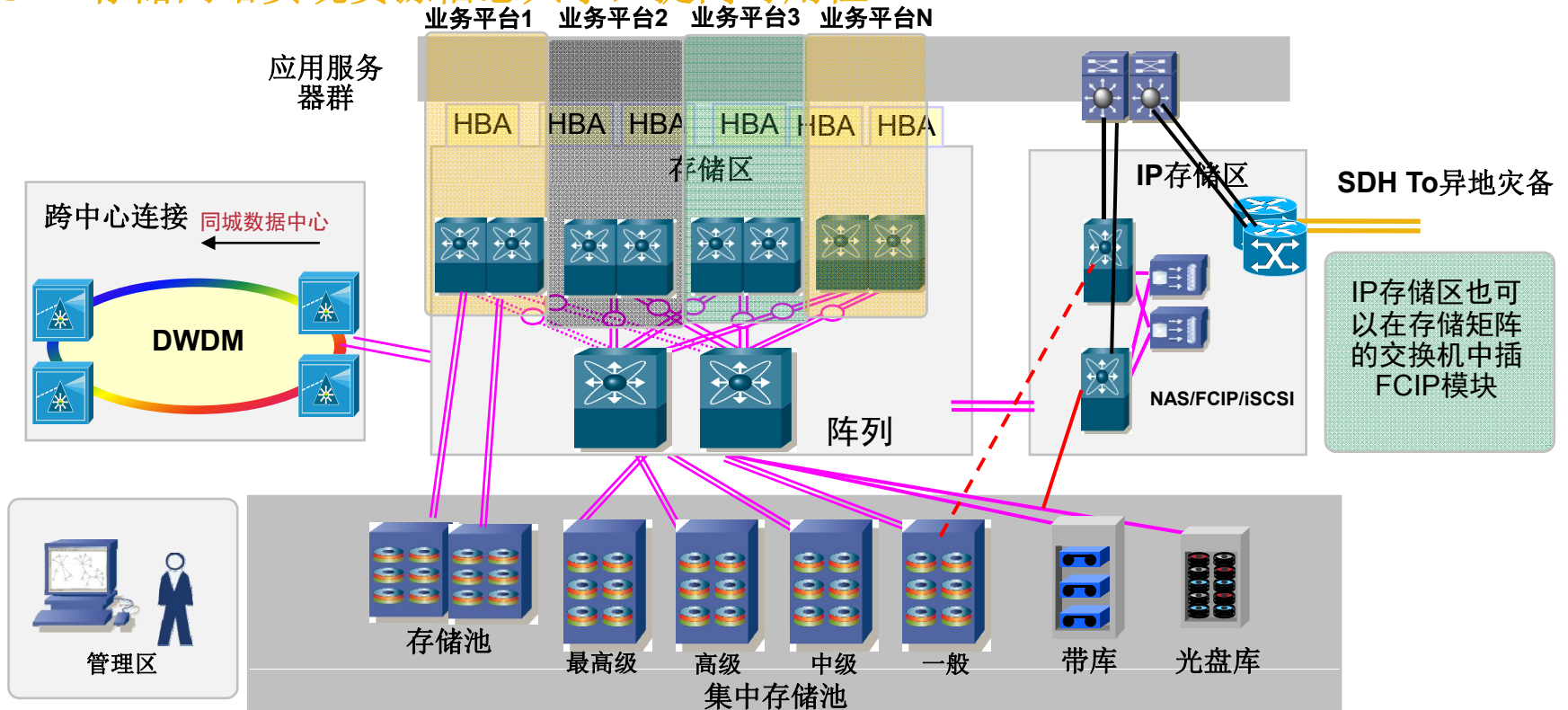


- 应用平台区：
 - 采用双阵列、每个阵列双核心结构，保障高可用性
 - 边缘设备与核心设备可采用多条链路捆绑连接，实现低超载比
 - 集中存储池按服务等级分类
- 利用虚拟SAN实现网络分区，提高可用性
- IP存储区：单独分区，初期可以考虑与存储阵列整合。
- IP存储区可部署压缩加速设备，利用FCIP技术实现异地灾备。
- 管理区：对存储网络及存储资源进行管理、调配
- 同城灾备：通过DWDM连接同城数据中心或灾备中心
初期可以部署阵列A,将来扩展时再部署阵列B




数据中心存储架构设计 – 现阶段

利用SAN存储网络实现资源信息共享，提高可用性



- 通过SAN架构,利用虚拟SAN技术进行整合,实现存储网络分区,提高可用性
- 把多个SAN 孤岛集中到一个单一的交换架构中
- 降低了设备的投资及管理的复杂度
- 统一的存储管理
- 可集中进行灾难恢复计划:通过FCip技术实现异地容灾的部署, IP存储区也可以在存储矩阵的交换机中插FCIP模块,节约成本
- 对于不考虑虚拟存储技术的系统,则需要考虑多台物理交换机
- 对于特殊要求存储业务(如上市公司特殊要求),可以独立部署SAN网络系统
- (注:具体设备部署需要根据存储和服务需要以及FC端口而定)

图例

-  存储交换机
-  以太网交换机
-  压缩加速设备
-  存储设备

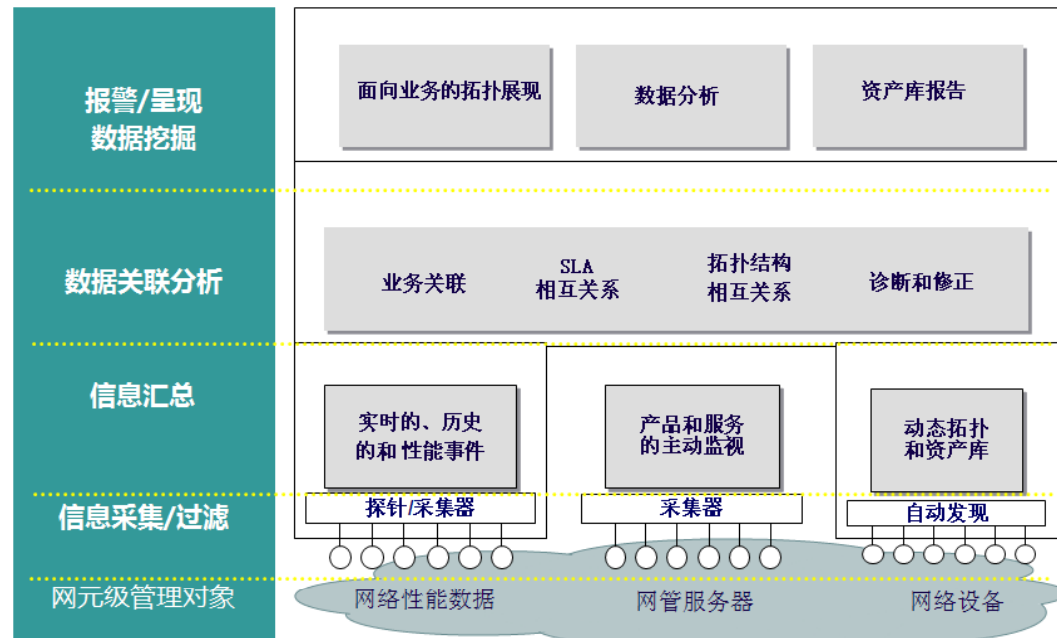


- 数据中心网络详细设计
 - 交换核心设计
 - 服务器区域设计
 - 广域网区设计
 - 企业边界区域设计
 - 数据中心员工接入
 - 开发测试区设计
 - 数据中心容灾和存储
 - 网络运维管理



数据中心网络管理-功能设计参考

- IT服务流程管理
- 安全运维管理
- 系统管理/机房管理
- 网络和故障信息管理
 - 拓扑管理和资产管理
 - 流量管理
 - 故障和告警管理
 - 配置管理
 - 性能管理
 - 报表管理
 - 日志采集和管理
 - 操作界面和接口



日常网络维护的得力助手

网元和事件为管理基础，全面的采集手段
高效处理、压缩、整合事件
事件关联分析
主动预警、趋势分析
统一、可定制呈现界面



COMBAT-LAB

- **带外管理，也称为OOB. (Out-of-Band) ，其作用是**
 - 提高运营效率（维护人员不需频繁到机房内部操作）
 - 显著减少宕机时间—(对系统可靠性有很正面的影响)
- **带内与带外管理共存/互补关系**
 - 带内网管: 常态下故障管理、事件管理、配置管理、变更管理和性能管理
 - 带外网管: 配置更改、故障排错和紧急访问手段

带外网管是保证网络99.999%可用性的有效手段



COMBAT-LAB

- 网络设备审计信息收集备案
 - 登陆、命令、配置信息
- 基于角色的网络设备运维管理
 - 层次化技术支持团队
- 备品备件支撑
 - 企业自建备件库
 - 思科齐全备品备件支撑服务的协助
- 网络设备软件版本标准化及入网机制的建立
 - 思科高级专业服务协助下的IOS软件版本评估、推荐、管理
- 网络设备配置标准化
 - 思科高级专业服务协助下的设备配置标准化、优质化
- 定期网络健康检查
 - 网络单点故障风险点分析
 - 网络链路、设备健康状况评估
 - 主动网络风险点改进及变更技术支撑



变被动响应为主动优化

注: 经验来自思科内部



数据中心运维管理模块设计参考

运维管理需要建立一个统一管理平台来提高管理水平，需要在技术、流程和组织架构/人员等多方面考虑，从技术平台上应该考虑：网络和故障管理，安全运维管理，系统/应用/数据管理，环境/机房，以及IT服务流程管理管理等。

