HUAWEI ENTERPRISE ICT SOLUTIONS A BETTER WAY

华为大企业基础网络解决方案技术主打胶片（园区网）

Author/ ID: 陆震 luzhen@huawei.com
Dept: 大企业SDT
Version: V100R001C00

enterprise.huawei.com
HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

目录

全球化IT整合是大企业全球化运营趋势

大企业全球化IT整合之路

IT系统分散、孤立

- 区域化运营，分散式管理
- 区域发展不平衡
- 总部无法有效监控运营
- 内部先进实践无法共享

分散运营模式

本国IT系统整合

- 全国统一IT战略
- 全国的流程实现一体化、结构化、标准化
- 统一IT系统实现有效运营监控

本国集中运营

IT系统海外覆盖

- 海外业务增长，运营模式改善
- IT系统海外部署
- 局部区域实现一体化管理

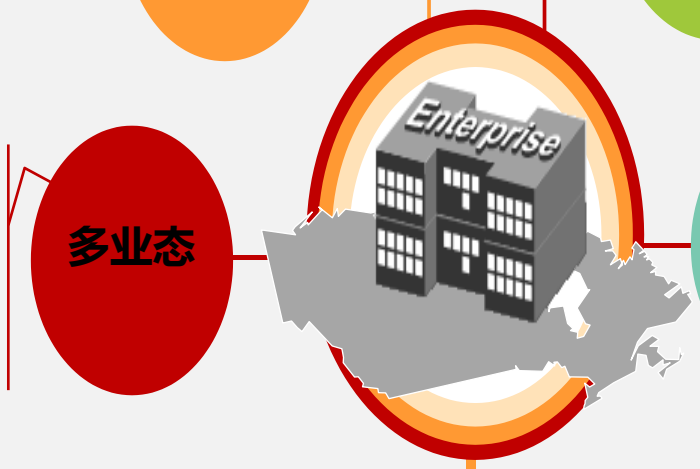
国际化运营

全球化IT整合

- 全球化IT战略
- 集团化运营
- 高可用的应用和IT基础设施
- 支撑以客户为中心的端到端流程集成

全球化整合运营

全球化整合运营大企业的特点和管理特征



全球化

➢ 多地域，一国为主，全球市场，跨国经营
➢ 多种经济、贸易、会计、税务、劳务制度

IT系统复杂

➢业务流程多，IT系统多
➢ 业务流程变化多，IT系统升级变化快

多业态

➢ 多级管控，多元化产业
➢ 业务组织单元多、形态多，变化频繁

成长性

➢ 国内高端企业还处于一个高成长期、快速发展期
➢ 企业转型、升级、并购、拆分、管理模式变化等较多

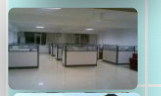
多组织

➢组织间业务关系复杂
➢组织间管理关系复杂

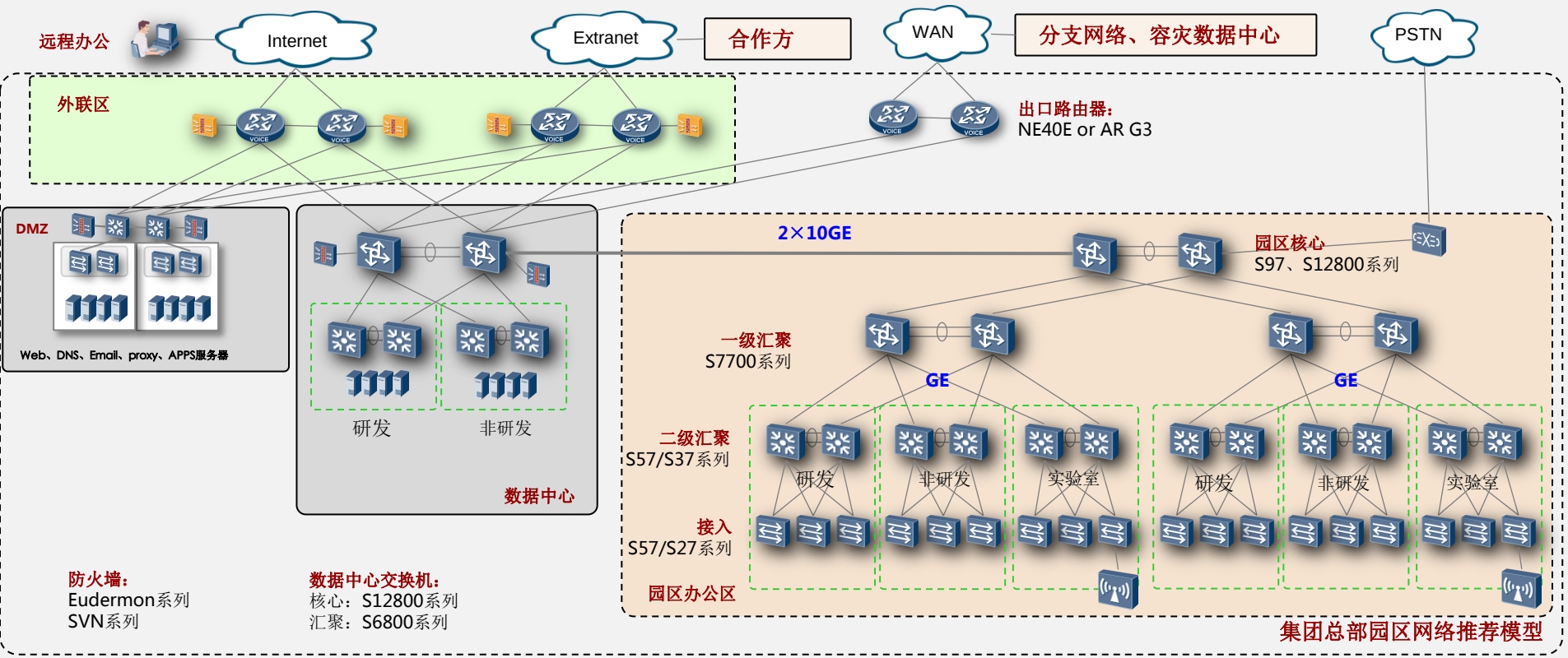
这些特点对网络架构设计和网络管理规范提出新的挑战 ，忽略网络将难以支撑企业全球化整合运营。

HUAWEI

园区网场景概览

	总部	集团企业总部园区一般为大中型园区，是一种高密度的非运营网络，在有限的空间内聚集了大量的终端和用户，是企业各分支机构的汇聚中心。
	区域中心	地区总部一般为中小型园区，作为集团企业在当地的运营中心，承担着企业本地化开发设计销售等众多业务，是企业本地化的重要的地区中枢。
	办事处	办事处一般为小型园区，用户与终端数量较少，主要支撑集团企业在当地开展业务。
	普通办公区	普通办公区终端以PC（云桌面）和通讯设备为主，终端密度较大，用户除公司员工外也会包括一些访客（合作方和客户）。
	高安全办公区	高安全办公区一般适用于集团企业设计部门或者竣工企业，对企业信息安全有特别严格要求，终端以PC（云桌面）和通讯设备为主，终端密度较大。
	访客区	访客区主要是集团企业接待合作伙伴和客户的区域，网络以方便灵活为主，既满足访客的Inetrnet访问需求又能保证企业信息不泄露。
	实验室	开发实验室主要涉及企业与客户或者合作伙伴的联合测试、新业务上线测试等场景，需要保证与客户或者合作伙伴的网络互通，又要避免影响整个企业网络。
	会议室	会议室内拥有语音终端、视频终端等多种终端设备，会议室网络既要保证与会人员的方便接入，同时又要保证会议质量。
	生产环境	生产车间（仓库）一般环境恶劣，涉及PC、工控机、监控设备、生产终端等多种终端设备，而且生产网络需要保持一定的独立和高的稳定可靠性保证安全生产。
	物流园区	物流园区以大型仓库为主，车辆货物进出频繁，终端以PDA设备、监控设备为主。整个园区网络要体现便捷、广覆盖。

总部园区网络



□总部园区需求

✓集团总部是整个集团企业网络的交汇枢纽，汇总所有分支和办事处，集团总部也是研究中心等大型园区网络的汇集地，网络流量较大；且各种业务流量汇集，容易形成拥塞和干扰；

✓集团总部的职能部门较多，需要按照职能部门的网络分区和安全隔离

✓集团总部为整个公司的网络核心，对可靠性要求较高；

□解决方案

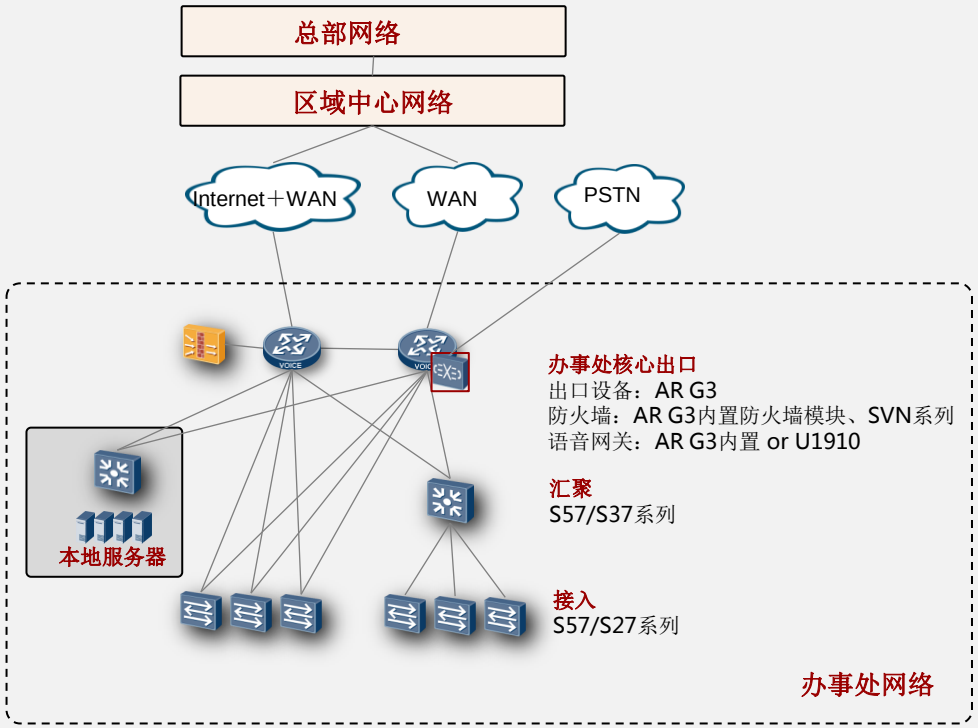
✓网络架构：分层组网，接入层＋汇聚层＋核心层＋出口路由器，并分区汇聚，层次清晰，结构清楚，管理维护方便

✓分区：在网络汇聚层面分为办公、DMZ、数据中心等几个汇聚区域，每个区域都有自己的汇聚交换机；网络内部按部门划分多个虚拟网络（VPN）

✓核心汇聚网采用双链路、双节点的可靠性树形拓扑架构，链路和节点冗余，保证网络的可靠性；

✓网络出口Internet访问路由器和企业内网互联路由器（WAN）分开，互不干扰

办事处网络



□办事处网络需求

✓规模：办事处有大有小，20～400信息点；

✓经济性：办事处网络的出口不宜租用昂贵的专线，办事处内部网络也不建议双节点、双链路组网模式

✓总部互联：办事处网络的内部业务需要接入总部和区域中心的内网区；

✓Internet访问：办事处的出口有访问Internet的需求，需要进行地址翻译和防火墙设置

✓本地服务器：时延比较敏感的企业应用，为了保证业务及时顺畅，需要在办事处内部部署本地服务器

✓可靠性：办事处的网络可靠性要求低于总部和区域中心网络

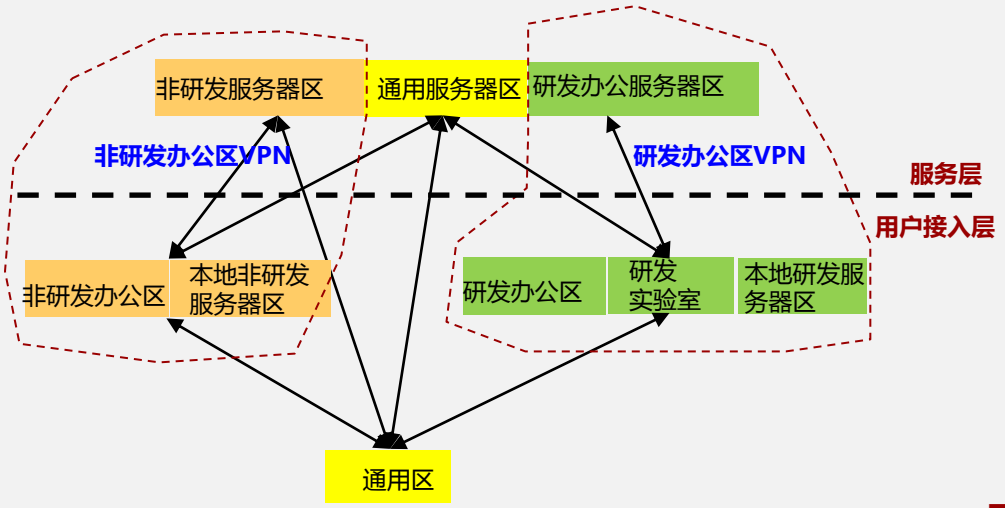
□办事处网络解决方案

✓采用专线作为内网互联的链路，InternetVPN作为备份链路，节省互联费用，保证网络可靠性，出口路由设置防火墙策略保证网络安全

✓Internet访问流量和内网互联流量在出口分开，互不干扰；

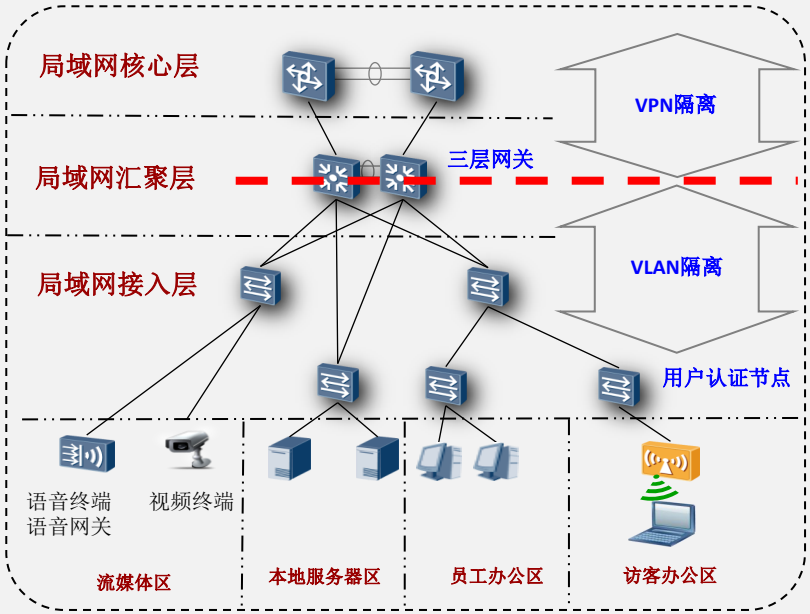
✓Internet访问如果直接从办事处出口，需要在办事处出口部署防火墙设备或者模块；如果通过区域中心统一出口，则需要通过隧道把Internet访问流量连接到区域中心的Internet出口路由器；

普通办公网络



普通办公区网络需求

- ✓根据用户身份认证确定网络使用权限
- ✓不同的部门需要隔离和受控互访
- ✓需要为访客提供网络服务，但需要与员工的网络隔离
- ✓千兆到桌面，平滑扩展，支撑未来桌面云应用
- ✓语音、视频等流媒体业务与数据业务并存
- ✓网络可靠性，保障业务系统可用



□普通办公区安全认证的解决方案

✓接入层交换机上进行用户身份认证，认证方案有两种模式：

➢一、动态ServiceVLAN：用户初始接入GuestVLAN，根据用户认证的身份，下发用户归属的ServiceVLAN，在三层网关上映射不同的部门VPN；由于用户认证前后改变了VLAN，需要重新二次分配IP地址；

➢二、在物理位置上划分隔离区域：用户认证的目的为验证用户是否有接入该区域的权限，不更改用户的VLAN

✓语音、视频等哑终端采用MAC认证模式，以防止有人冒用这些设备的接入端口；为保证这些业务的QoS，给这些终端接入的端口分配VoiceVLAN

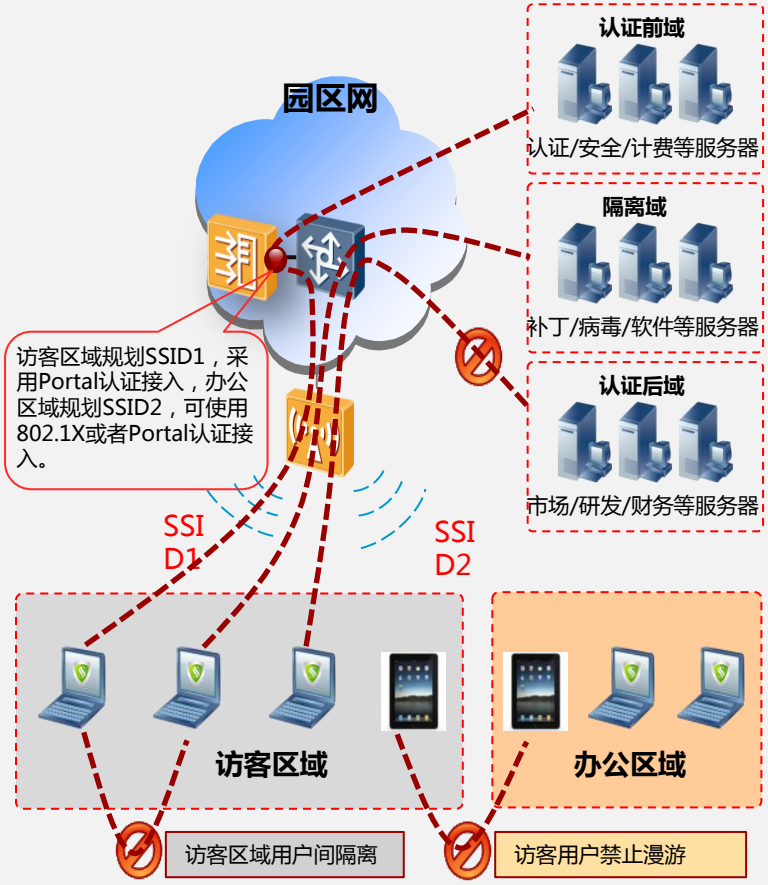
HUAWEI

访客办公区

外部访客管理网络需求

✓访客是指企业外部客户、合作方员工等人员，对于该类终端，其网络权限不同于内部员工，需要加以限制。

✓访客大多为移动办公，区域一般采用无线WLAN方案。



解决方案

✓无客户端Portal认证

访客终端采用Portal无客户端方式，方便用户接入。

✓公共帐号管理

给访客分配临时账号，考虑到管理员会面临大量开户、销户和帐号发放的操作，可在用户管理系统中规划公共帐号管理模块，减轻管理工作量和提升客户体验。

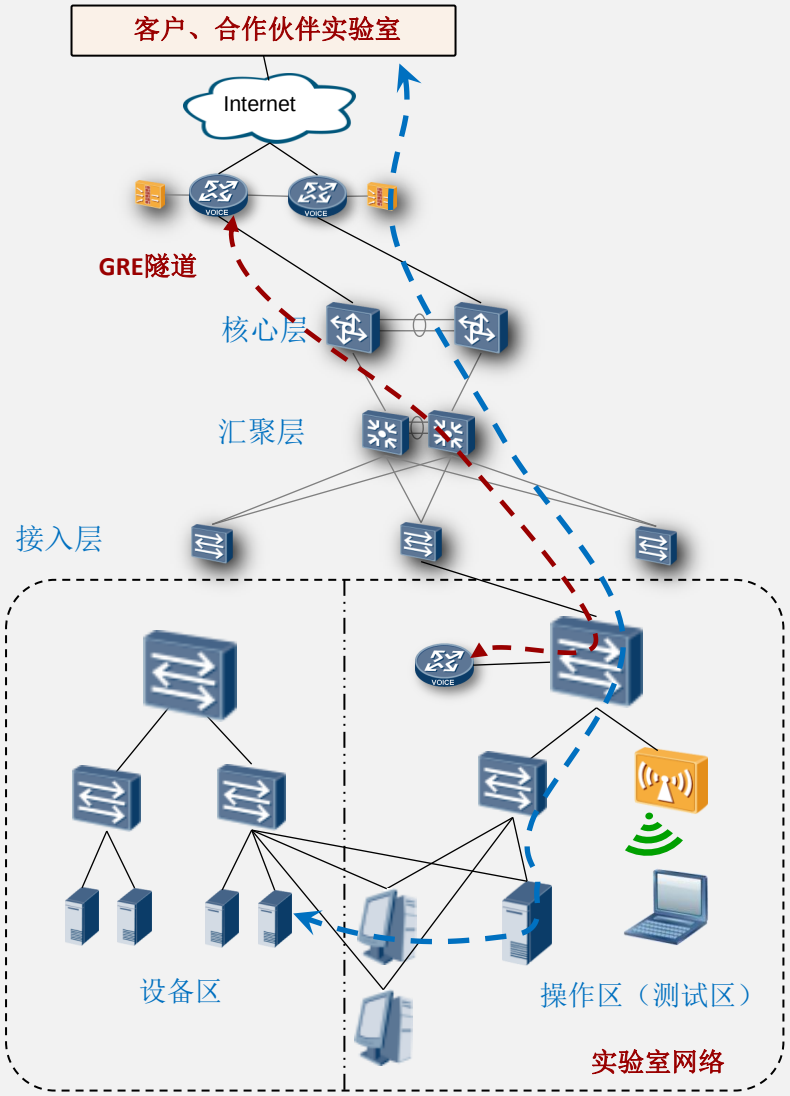
✓开放特定服务资源

对于访客，可只开放Internet和隔离域资源，禁止访问认证后域的企业内部资源。

✓用户隔离

对于无线客户，漫游存在很大安全隐患。可通过规划特定SSID，限制访客漫游到办公区域；另外，可通过二层隔离技术，限制访客之间互访。

实验室（开放实验室）网络



实验室网络需求

✓实验室网络相对独立，需要单独的Internet出口实现Internet上网测试以及与合作伙伴或者客户实验室之间的网络互通

✓实验室网络的测试环境不能影响办公网络

✓避免测试网络造成信息泄露

✓测试操作区的无线设备操作

解决方案

✓实验室操作区，与研发办公区进行虚拟网隔离，三层网络设置独立的研发实验室VPN，二层网络实验室操作区与研发办公区使用不同的VLAN

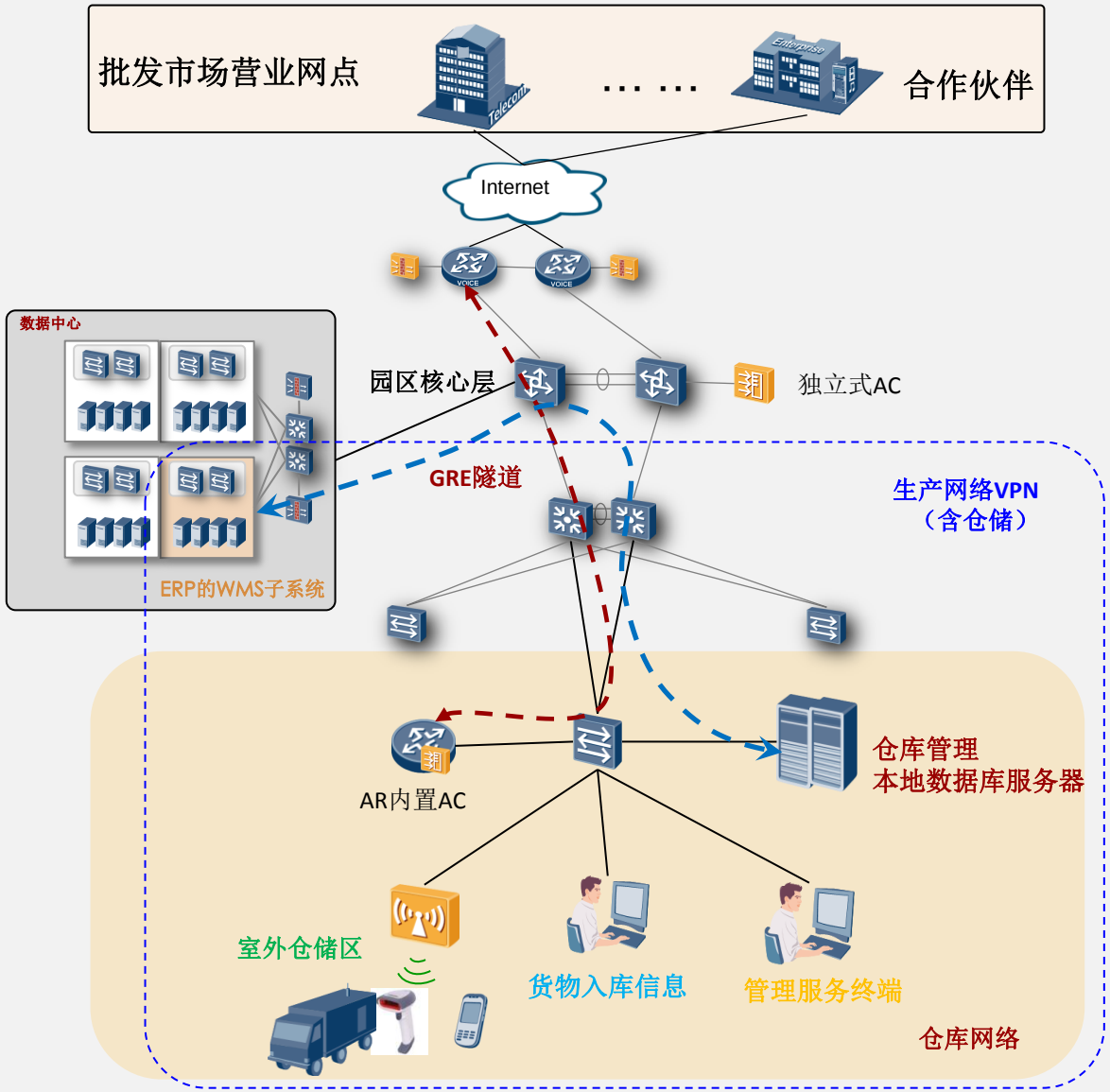
✓实验室设备区，使用单独的小网，与大网不通；操作区工作站和服务器采用双网卡连接设备区和操作区；

✓实验室GRE隧道连接到园区出口路由器，为实验室提供Internet出口，在需要Internet访问的实验室中配置一台路由器，由该路由器打GRE隧道到园区Internet出口路由器，该隧道的防火墙策略在出口路由器上实现；

✓实验室操作区（测试区）建议采用二级接入，设备选用千兆交换机，交换机较多时，使用一台交换机汇聚其它交换机；

✓实验室根据情况采用有线无线融合方案，保证实验方案灵活性；

仓库网络



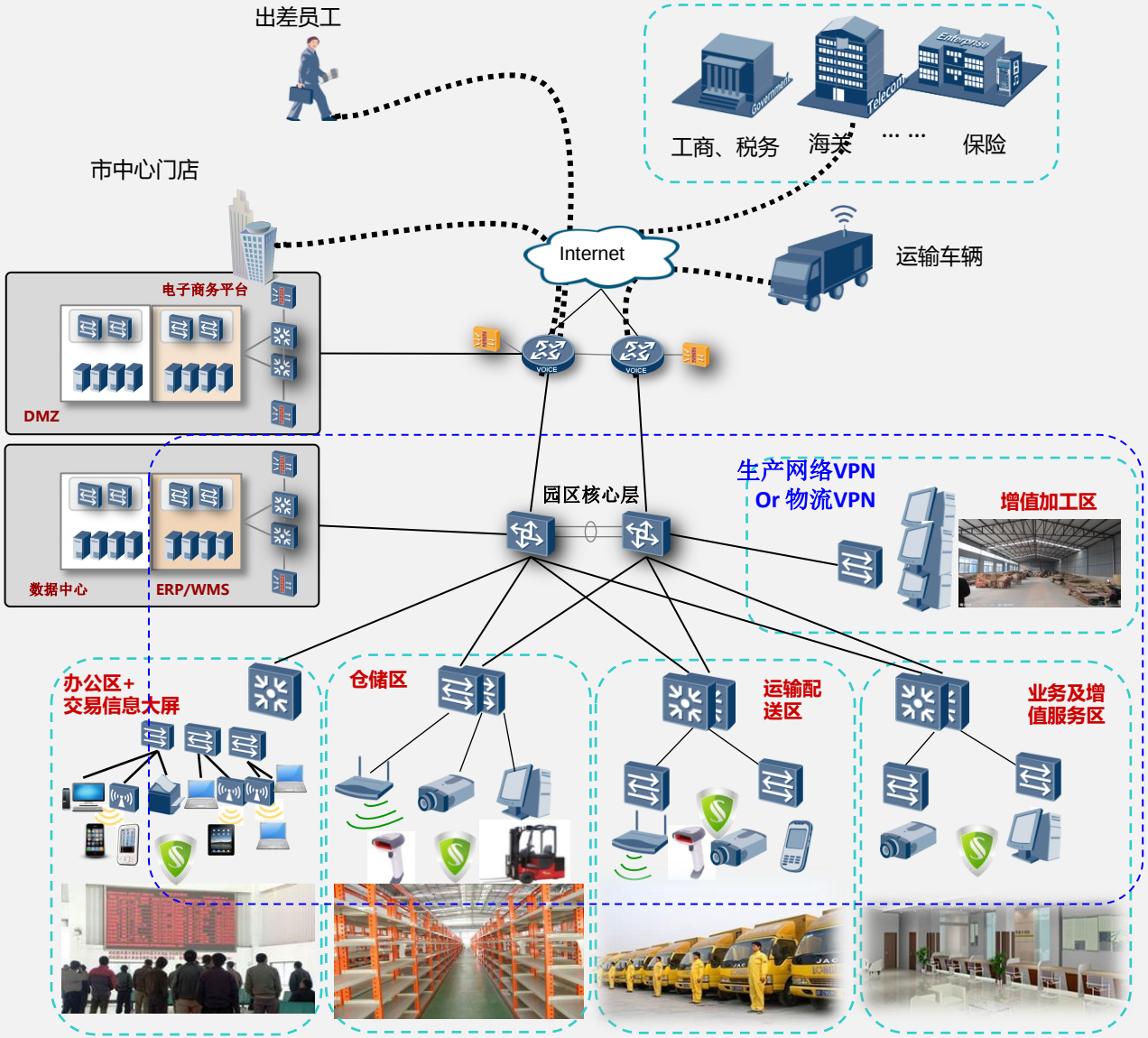
仓库网络需求

- 入库货物的入库、储存、盘库管理
- 与远程的批发市场和合作伙伴互通；
- 与数据中心ERP－WMS数据互通；
- 移动盘库管理
- 工业级设备保障
- 网络运维简单，设备维护方便

仓库管理解决方案：

✓将仓库网络和数据中心的ERP（含WMS）服务器都纳入生产网络VPN；
✓仓库设置路由器通过GRE隧道连接Internet出口路由器，提供与外部批发市场和合作伙伴的互联通道
✓采用工业级AP作为仓库室外无线覆盖的接入设备：对于室内外仓储区的恶劣环境，推荐AP6510室外工业级AP支持802.11n无线接入点，高等级防尘防水标准，可适用于仓储配送区甚至冷冻仓储区，低温环境启动。
✓AC可以采用独立式AC，园区独立部署；也可以采用AR内置式AC，在仓库节点分布式部署；
✓有线无线一体化满足移动盘库等应用，并可根据业务量大小调整无线射频器数量，避免入库高峰的扎堆现象。

智慧物流园区



物流园区网络需求

- ✓移动盘货、点货服务
- ✓入园车辆管理、园内企业管理、缴费、信息发布等业务
- ✓与银行、工商、税务、报关、保险等外部机构互联
- ✓车源信息、货源信息的及时发布
- ✓及时响应订单配送需求
- ✓园区内各职能区域的网络隔离
- ✓安全网络交易

解决方案

- ✓通过VLAN或者VPN技术实现各职能区域的网络隔离
- ✓有线无线融合实现泛在覆盖，实现移动盘库、车辆定位、移动办公
- ✓数据中心承载WMS、TMS、电子商务、CRM、OA等系统，及时响应订单配送需求
- ✓有线、3G双链路备份、GE上行WAN口，双电源冗余，保证与外界通信的工商、税务、保险等重要信息的安全
- ✓网络带宽保障车源信息、货源信息及时发布
- ✓SSL VPN功能支持园外交易支持安全交易

HUAWEI

HUAWEI ENTERPRISE ICT SOLUTIONS A BETTER WAY