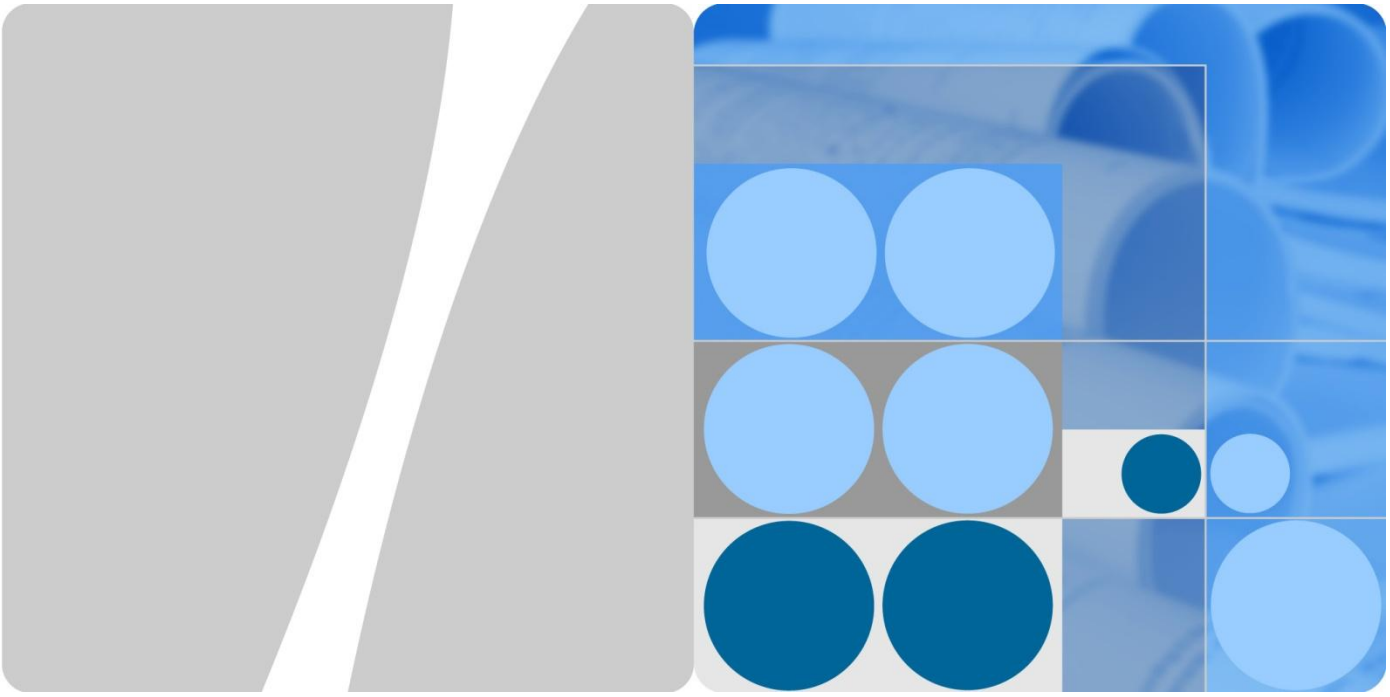


One Net Campus 金融行业园区网解决方案 V100R001C03

技术建议书

文档版本 01

发布日期 2012-08-30

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://enterprise.huawei.com

客户服务邮箱： ChinaEnterprise_TAC@huawei.com

客户服务电话： 400-822-9999

目录

1 概述

1.1 金融园区网承载业务及网络发展趋势

金融业是指经营金融商品的特殊行业，它包括银行业、保险业、信托业、证券业和租赁业。金融园区网一般是指金融企业内部 OA 网，一般独立于生产网，主要承载金融企业的办公、审计等数据、语音、视频业务，部分园区网络同时需要承载园区视频监控流量。

在信息化建设越来越深入的今天，随着大量智能终端的出现，以及无线通信技术的发展，金融园区网的网络发展具有如下趋势：

- 云计算+业务多样化

  视频会议、桌面云、高清智真等多媒体和云计算业务在企业园区的广泛应用，在促进企业生产办公效率和减少出差成本的同时，对企业园区网的网络带宽和质量提出了新的要求。

- 安全关注点向接入侧转移

  在网络安全方面，目前网络攻击方式已经从传统的外部渗透入侵方式逐渐转变为内部木马僵尸等病毒泄密。攻击方式的转变，使得企业网络安全关注的重点逐渐从网络转向用户。员工自身的行为监管是加强企业的信息安全的重要一环，预防真正的“内部攻击”。

- IT&IP 融合智能管理

  对于企业来说，网络管理也朝着多维度、智能化管理的方向发展，主要包括：

  园区智能管理： 一站式网管、基于业务的流量监管、快速问题处理

  园区安全策略： 多维接入认证、分权分域管理、文件管理、行为监管

  园区智能化建设： 智能能耗管理、快速部署、智能运维、机房精细化管理

1.2 金融园区网的建设要求

承载业务决定网络建设要求。因此，为了保证金融园区内视频监控、多媒体会议（甚至智真会议）等业务系统的正常运作，以及特别是越来越多的无线终端的接入需求，金融企业园区网络的设计需满足以下要求：

- 业务高 QoS 保障

园区业务多样多媒体化，智真、桌面云等业务要求更高的 QoS 保障和更优的用户体验。

- 园区大宽带

  桌面云、高清视频等业务驱动千兆到桌面时代，万兆园区网络。

- 支持移动办公网络

  需要支持有线无线一体化接入、一体化认证。

- 全方位安全保障

  由于现在网络威胁逐渐由外部渗透的攻击向内部泄密转变，无线接入方式要求更高的接入认证保障。

- 智能融合网管

  业务与设备多样化，网络需要支持更智能、更高效的网管平台，并能够融合管理园区各种 ICT 设备。

1.3 园区网设计原则

企业园区网是企业的业务信息平台，应本着以下原则进行建设：

- 超前性与实用性结合

  网络技术发展迅猛，如果设备缺乏先进性，设备可能很快落后甚至被淘汰，但也不能过分超前，以避免造成投资的浪费。为此，在网络建设中，需注意超前性与实用性结合，确保投资有效，使之能真正发挥出相应的作用。

- 安全性与可靠性

  在园区网建设中，安全性是整个网络建设中的重中之重，要通过各种技术确保系统应用的安全性。同时，要求系统本身具有高度的可靠性，这样才能保证网络客户的应用。

- 可管理性

  网络管理是一个长期的投资，在网络建设中对网络可管理是一项重要的应用原则，通过选择全网的可管理性软件，减少日常维护费用。

- 可扩展性

  企业网络不但需要能够满足当前需要，随着后续企业规模的扩大、技术的发展，未来网络需要承载更多的业务及提供更多的优质服务。所以，网络的可扩展性是网络建设中必须提前规划的重点。

2 金融园区网络总体设计方案

2.1 金融园区网总体网络架构

2.1.1 总体网络设计原则

对于企业而言，办公网络作为实现提升企业办公效率，整体增值的业务承载通道，网络的简单可靠、易部署、易维护是非常必要的。因此在金融园区网中，拓扑结构通常也以最常用的星型结构为主，较少使用环网结构。

基于星型结构的园区网设计，通常遵循如下原则：

- 层次化

  将园区网络划分为核心层、汇聚层、接入层。每层功能清晰，架构稳定，易于扩展和维护。

- 模块化

  将园区网络中的每个部门或者每个功能区划分为一个模块，模块内部的调整涉及范围小，易于进行问题定位。

- 冗余性

  关键设备采用双节点冗余设计；关键链路采用 Trunk 方式冗余备份或者负载分担；关键设备的电源、主控板等关键部件冗余备份。提高了整个网络的可靠性。

- 安全隔离

  园区网络应具备有效的安全控制。按业务、按权限进行分区逻辑隔离，对特别重要的业务采取物理隔离。

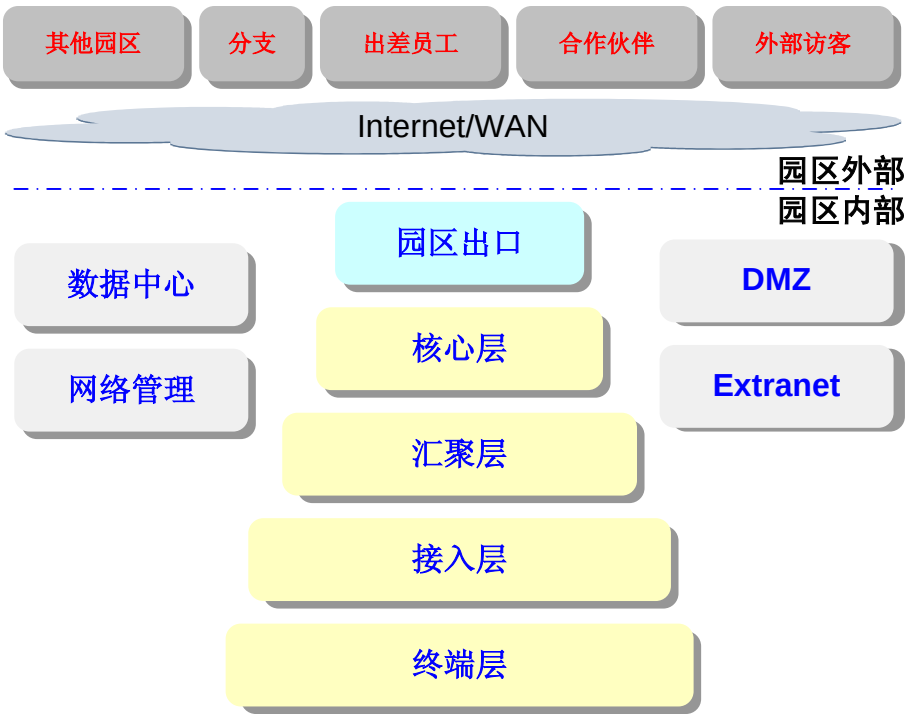
- 可管理性和可维护性

  网络应当具有良好的可管理性。为了便于维护，应尽可能选取集成度高、模块可通用的产品。

2.1.2 金融园区网总体网络逻辑架构

园区网络的逻辑架构如图 2-1 所示，包括五大部分。

图2-1 园区网络的逻辑架构



- 终端层

  包含园区内的各种终端设备，例如 PC、笔记本电脑、打印机、传真、POTS 话机、SIP 话机、手机、摄像头等等。

- 接入层

  负责将各种终端接入到金融园区网络，通常由以太网交换机组成。对于某些终端，可能还要增加特定的接入设备，例如无线接入的 AP 设备、POTS 话机接入的 IAD 等。

- 汇聚层

  汇聚层将众多的接入设备和大量用户经过一次汇聚后再接入到核心层，扩展核心层接入用户的数量。汇聚层通常还作为用户三层网关，承担 L2/L3 边缘设备的角色，提供用户管理、安全管理、QoS（QualityofService）调度等各项跟用户和业务相关的处理。

- 核心层

  核心层负责整个园区网的高速互联，一般不部署具体的业务。核心网络需要实现带宽的高利用率和网络故障的快速收敛。

- 园区出口

  园区出口是园区网络到外部公网的边界，园区网的内部用户通过边缘网络接入到公网，外部用户（包括客户、合作伙伴、分支机构、远程用户等）也通过边缘网络接入到内部网络。

- 数据中心区

  部署服务器和应用系统的区域。为企业内部和外部用户提供数据和应用服务。

- DMZ（Demilitarized Zone）区

通常公用服务器部署于该区域，为外部访客（非企业员工）提供相应的访问业务，其安全性受到严格控制。

- Extranet 区

  与 DMZ 区相似，但它主要是面向合作伙伴提供服务。

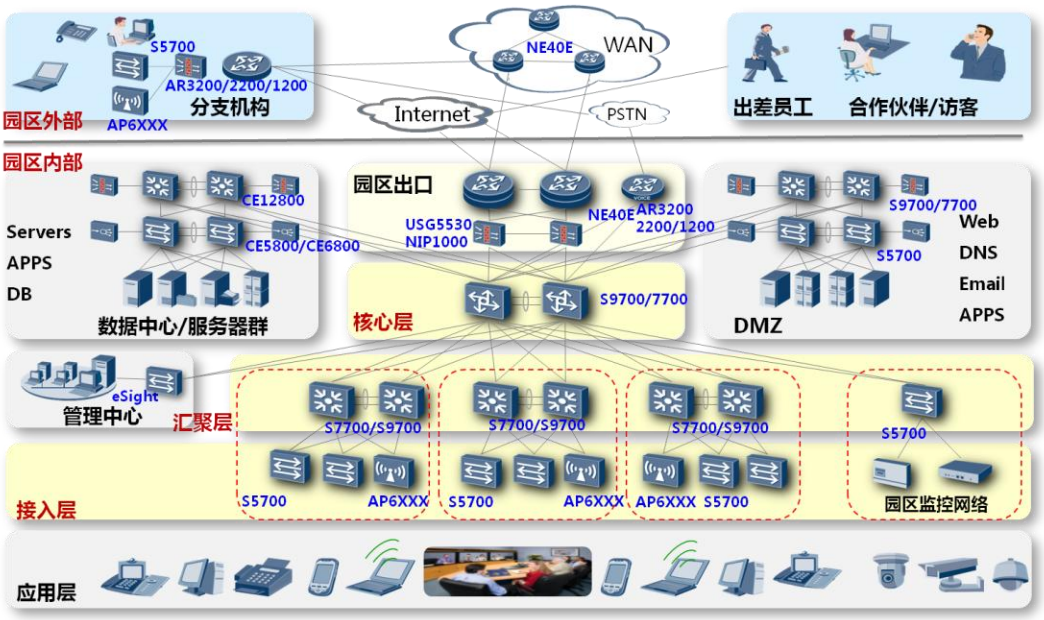
- 网络管理区

  对网络、服务器、应用系统进行管理的区域。包括故障管理、配置管理、性能管理、安全管理等。

2.1.3 金融园区网网络总体物理架构

为了满足云计算和多媒体业务广泛应用而带来的业务高 QoS 保障、大带宽、全方位安全保障、支持移动办公、智能融合网管的需求，对应逻辑架构，华为万兆金融园区网的物理架构如图 2-2 所示。

图2-2 园区网络的物理架构

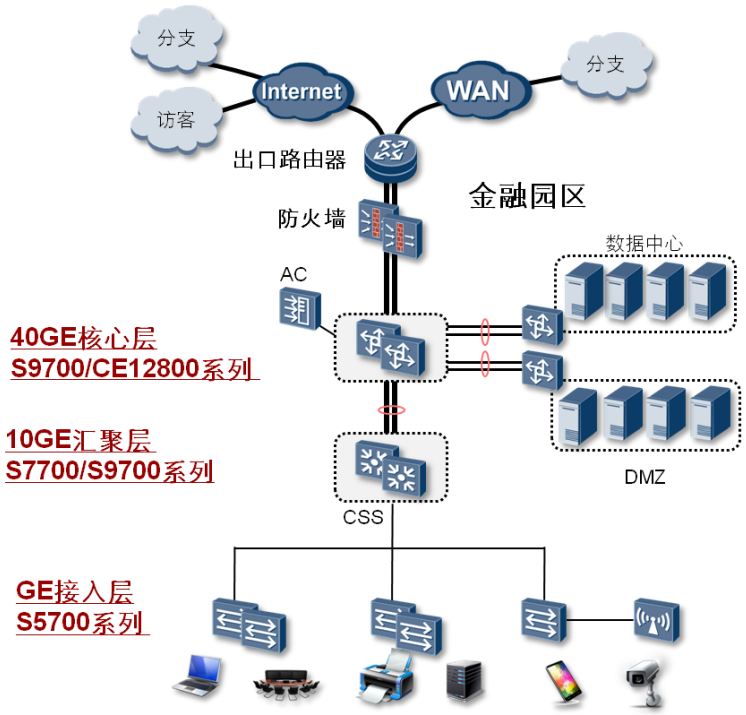


该组网结构具有如下特点：

- 以核心节点为“根”的星型分层拓扑，架构稳定，易于扩展和维护。
- 各部门和功能分区模块清晰，模块内部调整涉及范围小，易于进行问题定位。
- 双节点冗余设计，关键链路均采用 Trunk 链路，保证网络的可靠性。
- 支持各种业务终端接入，一张 IP 网络承载所有业务。
- 支持分支接入、员工远程接入、合作伙伴接入、外部用户访问等各种外联场景。

按照出口、核心、汇聚、接入模型结构，该组网结构可以简化为如下图所示：

图2-3 华为金融万兆园区网络架构图



2.2 核心区网络规划

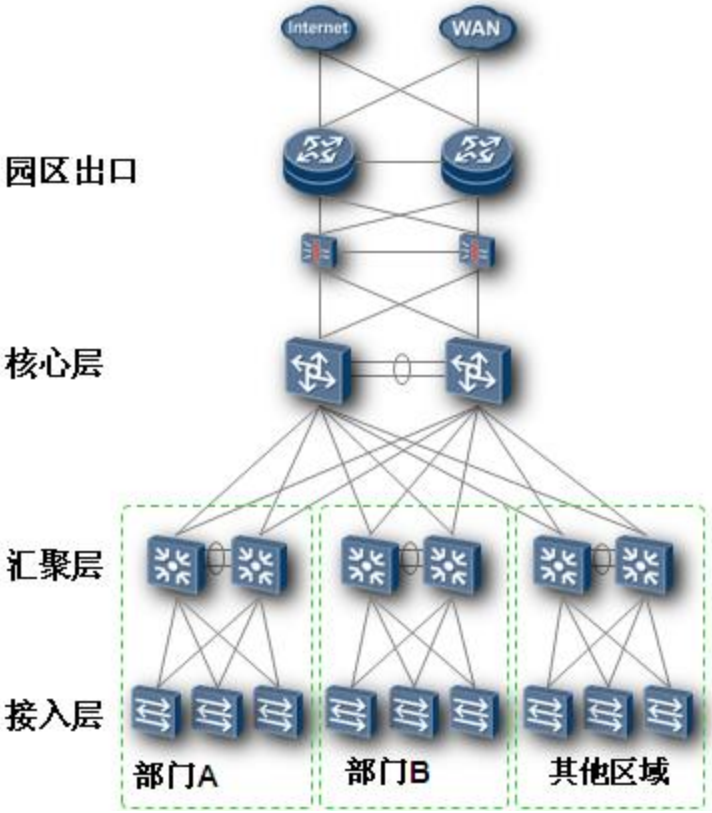
核心区是整个园区网络的枢纽，连接着园区内的各个区域。承担了内部数据流量和对外数据流量，在逻辑上成为可靠性、安全设计的中心。

2.2.1 物理组网规划

如图 2-4 所示，核心区域建议采用园区出口、核心层、汇聚层和接入层的架构模型，具有如下的优势：

- 层次化设计：核心层、汇聚层、接入层，每层功能清晰，架构稳定，易于扩展和维护。
- 模块化设计：每一个模块一个部门，部门内部调整涉及范围小，定位问题也容易。
- 冗余性设计：双节点冗余性设计，适当的冗余性提高可靠性，过度的冗余不便于运行维护。
- 对称性设计：网络的对称性便于业务部署，拓扑直观，便于设计和分析。

图2-4 核心区域组网结构图



园区网核心区的星型设计使得网络架构简单，易于维护和部署。但星型不等于不成环，仍然需要运行破环协议，推荐使用 MSTP 协议。

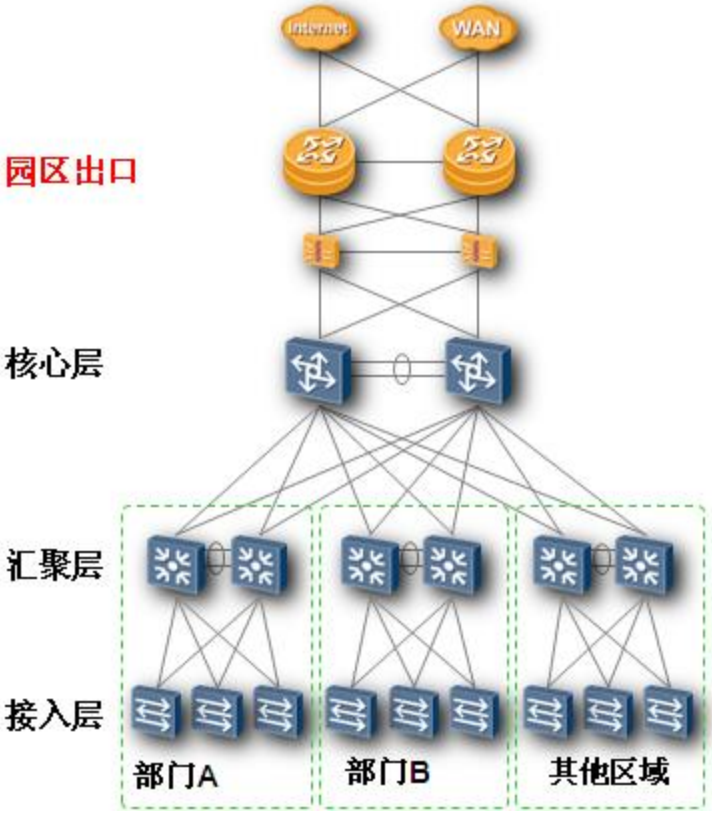
园区出口设计规划

园区出口指企业接入广域网和 Internet 的出口，园区出口的主要功能是外部的互访，包括企业分支、出差员工、合作伙伴/访客的访问，具体内容请参见《互联区网络规划》。

Internet 网络的安全性低、可靠性低、费用低，WAN 安全性高、可靠性高、费用高。为保证 WAN/Internet 链路的高可靠性，可申请两条链路，实现冗余备份，也可以 WAN 作为主用链路，Internet 作为备份链路。

园区出口网关需要配置防火墙、IPS 等，根据不同的安全性要求和投资规模选择安全部件。

图2-5 核心区域组网结构图-园区出口



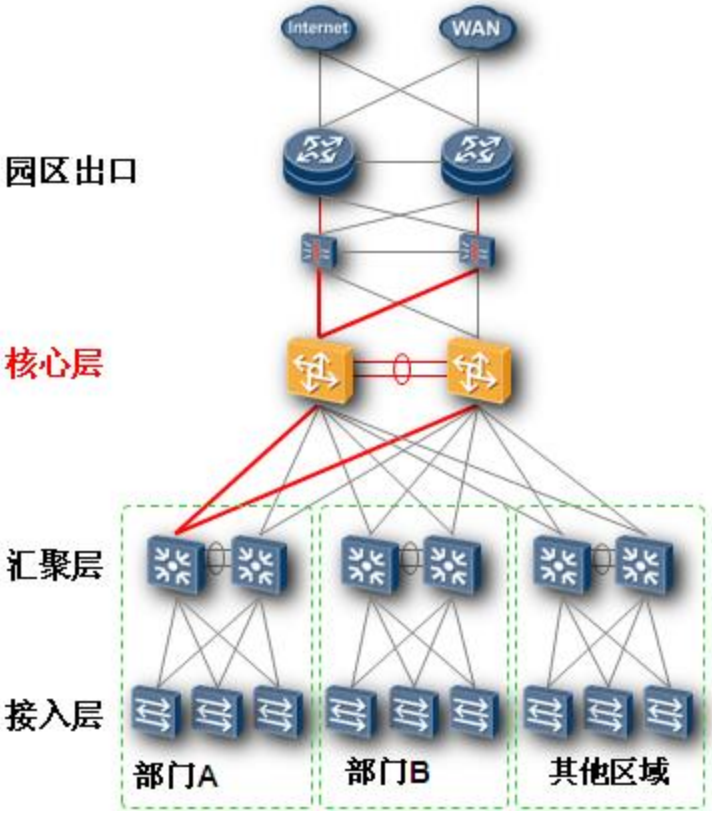
核心层设计规划

核心层部署园区的核心设备，连接所有的汇聚交换机，转发各个部门之间的流量。核心层对三个以上部门规模的企业来说是必须的，除了减少连线、路由 Peer 之外，让扩展以及日常策略调整也变得简单。

通常情况下，核心层需要采用全连接结构，保持核心层设备的配置尽量简单，并且和业务部门无关。

核心层设备需要具有高带宽、高转发性能，否则将无法支撑企业内外部的业务流量。

图2-6 核心区域组网结构图-核心层

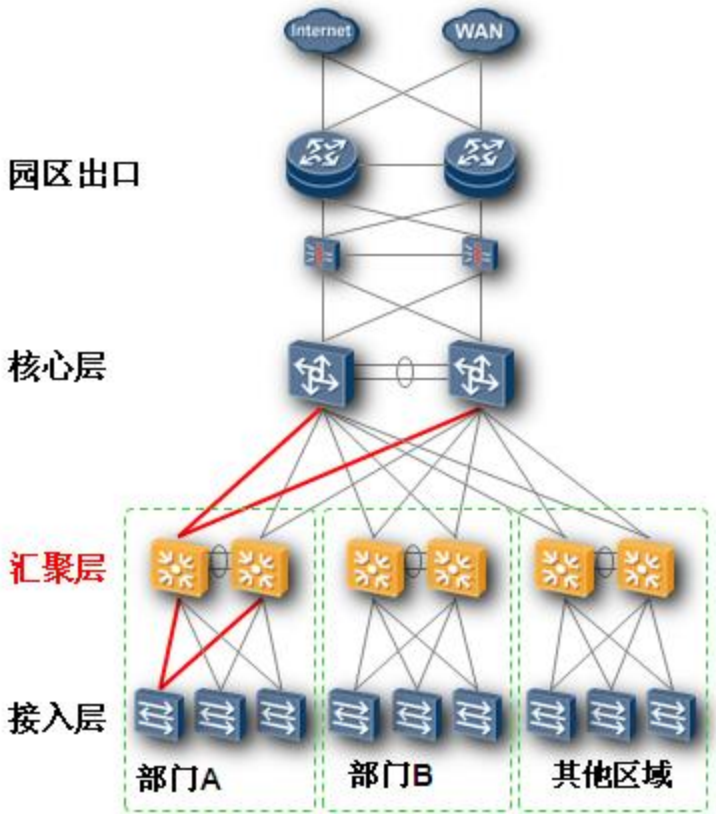


汇聚层设计规划

汇聚层是部门的核心，转发部门用户间的“横向”流量。同时提供到核心层的“纵向”流量。对接入层隐藏核心层，作为园区网的配线架，将大量用户接入到互联的网络中，扩展核心层设备接入用户的数量。

如图 2-7 所示，汇聚层需要双归到核心层并支持接入层的双归接入。通常汇聚层承担着L2/L3 边缘的角色，需要具有高带宽、高端口密度、高转发性能等特点，用于支撑该汇聚层下各业务部门之间的流量。

图2-7 核心区域组网结构图-汇聚层

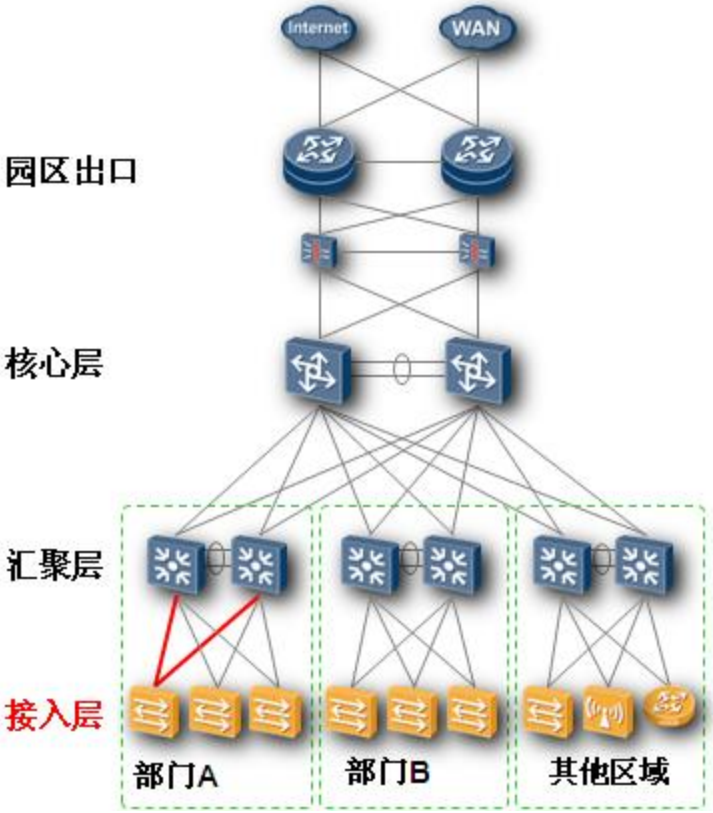


接入层设计规划

接入层是最靠近用户的网络，为用户提供各种接入方式，是终端接入网络的第一层，一般部署二层设备，双归属到汇聚层两个不同的交换机。接入层除了需要部署丰富的二层特性外，还需要部署安全、可靠性等相关功能。

接入层需要具有高端口密度，以支持更多的终端接入园区网络。

图2-8 核心区域组网结构图-接入层



2.2.2 可靠性设计规划

从上述组网图可以看到，网络可靠性由双设备、链路冗余来保证。

对于双设备、链路冗余的网络，如果接入层进三层，在接入层和核心层之间采用三层路由的方式，通过等价路径再辅助部署 BFD（Bidirectional Forwarding Detection）快速检测故障，就能够保证链路故障、设备故障的快速切换，同时也能够充分利用冗余链路。

更多的组网方式是在汇聚层进三层，这样就需要解决接入层和汇聚层之间二层流量的环路问题。传统的方案是 STP＋VRRP 的方案。该方案通过阻塞某些链路的转发实现二层破环，虽然该方案采用了标准的协议，支持多个厂家设备的混合组网，但是其缺点也是显而易见的：

- 收敛时间

  传统的 STP（Spanning Tree Protocol）技术收敛速度慢，在故障发生时，故障收敛时间>10 秒；虽然采用 RSTP 进行优化，但收敛时间任是秒级，秒级的业务中断，会导致较差的用户体验。

- 链路利用率低

  如果同一机架内的服务器属于同一 VLAN，则有一个上行链路的带宽无法利用。带宽利用率只有 50%；虽然 MSTP 基于 VLAN 进行优化，但不能从根本上解决问题。

- 配置维护复杂，网络故障率高

每个接入交换机和汇聚交换机都需要运行 STP 协议，随着接入交换机的增加，交换机需要处理的 STP 也越来越复杂，会导致可靠性问题。

我们推荐采用集群+堆叠的无环网络方案来解决上面的这些缺陷。核心、汇聚采用两台框式交换机集群。接入层采用盒式交换机，盒式交换机每两台堆叠。接入层交换机和核心/汇聚层交换机间的链路进行链路捆绑。

这个方案有四大优势：

- 简化管理和配置
  - 首先，集群和堆叠技术将需要管理的设备节点减少一半以上。
  - 其次，组网变得简洁不需要配置复杂的协议，如：STP/SmartLink/VRRP 等。
- 快速的故障收敛

  链路故障收敛时间可以控制在<10ms，大大降低了网络链路/节点的故障对业务的影响。
- 带宽利用率高

  采用链路 Trunk 的方式，带宽利用率可以达到 100%。
- 扩容方便、保护投资

  随着业务的增加，当用户进行网络升级时，只需要增加新设备，而不需要更改网络配置。平滑扩容，很好的保护了投资。

该方案极大提高了可靠性，以单链路故障率为 1 小时/1 千小时为例，增加到两条链路，就可以将故障率降低到 3.6 秒/1 千小时，可靠性从 3 个 9 提高到 6 个 9。

可靠性的另一个重要方面是设备可靠性，核心区设备一般为框式设备，在可靠性方面的要求包括：

- 支持主控单元的备份
- 支持电源模块的备份
- 支持模块化的风扇设计，支持单风扇失效
- 支持所有模块的热插拔

2.2.3 安全性设计规划

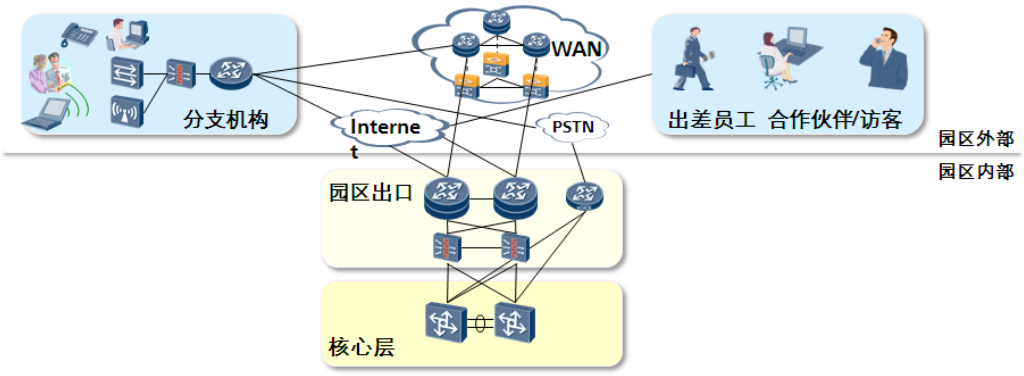
核心层与园区出口部署防火墙设备，主要解决如下几个安全问题：

- 园区内、外网之间的访问控制，实现园区内、外网的安全隔离。
- 企业分支与园区内网的访问控制，实现企业分支和园区内网业务的安全隔离。
- 出差员工与总部 DMZ 区的访问控制，实现出差员工与园区内网的安全隔离。
- 合作伙伴/访客与总部 DMZ 区的访问控制，实现合作伙伴/访客与园区内网的安全隔离。

2.3 互联区网络规划

2.3.1 物理组网规划概述

图2-9 互联区域网络

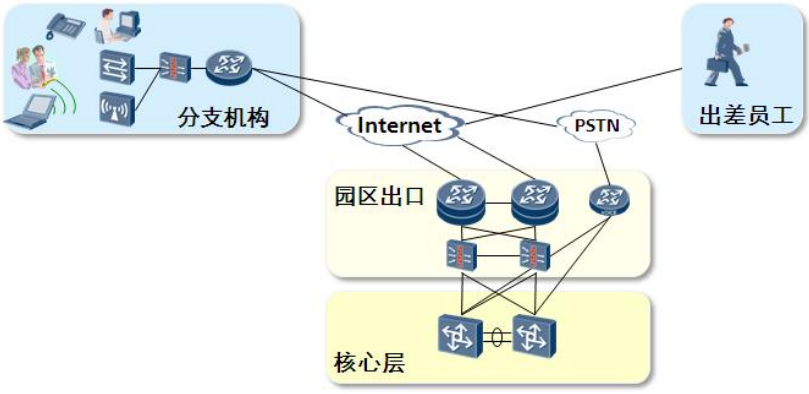


根据接入类型及服务类型划分多个不同的互联接入区域：

- Internet 互联
  企业外部用户（例如企业分支、出差员工等）通过 Internet 访问园区。
- Extranet 互联
  合作单位用户通过广域网或局域网访问园区。
- Intranet 互联
  企业内部用户访问园区内部及数据中心。

2.3.2 Internet 互联

图2-10 Internet 互联区域的网络架构



Internet 互联区包括路由器、UTM 等设备。其中 UTM 至少要包括防火墙和 IPS 两项功能。

- 入侵检测系统 IPS 对掺杂在应用数据流中的恶意代码、攻击行为、DDOS 攻击等进行侦测，并实时进行响应。
- 防火墙在网络层面，过滤非法流量、抵御外部的攻击，保护内部资源。

防火墙和 IPS 本身都是重要的网络设备，而且其位置一般都是作为网络的出口。其位置和功能决定了防火墙和 IPS 设备应该具有非常高的可靠性。

为了保证 Internet 互联区域的可靠性，所有设备均需要成对部署，即：两台路由器，两台 UTM（至少含防火墙和 IPS）。

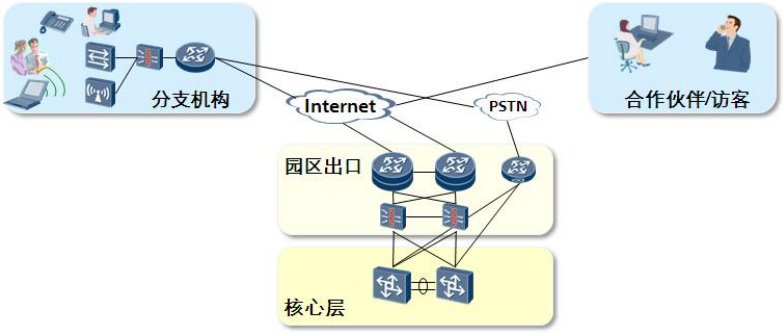
VPN 接入区根据需要提供 IPSec VPN 和 SSL VPN 两种接入功能，解决移动用户的安全接入问题。

- IPSec VPN 主要适用 Site-to-Site 方式接入
- SSL VPN 主要适用于 Client-to-Site 方式接入

可以部署独立的 IPSec VPN 网关和 SSL VPN 网关，也可以采用 UTM 设备统一接入。

2.3.3 Extranet 互联

图2-11 Extranet 互联区域的网络架构



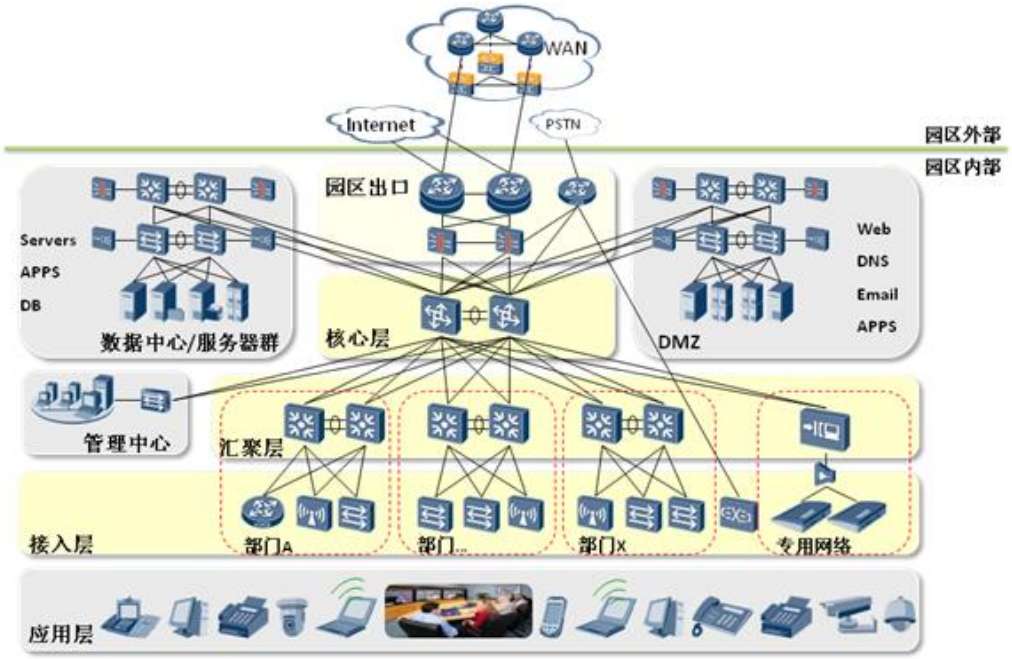
如图 2-11 所示，由于 Extranet 区域属于企业外部用户接入的区域，从网络信任关系上讲，安全等级与 DMZ 相同，都属于非可信网络，不能直接与园区连接。访问权限应限制在本区域内部及 DMZ 区域，内网访问应严格控制。

- 业务隔离：同 DMZ 区域，主要提供对外服务，因此对该区域网络应与内网隔离，必要的业务可以通过严格控制访问 DMZ 区域。
- 防火墙：在网络层面，通过 NAT 技术隐藏内网拓扑，保护内部资源控制访问权限。

2.3.4 Intranet 互联

企业内部用户访问园区内部或数据中心。

图2-12 Intranet 互联区域的网络架构



网络方面主要考虑线路双归，路由及设备的冗余备份。

需要部署独立的互联接入设备并部署 2 台进行热备，保证设备的可靠性。

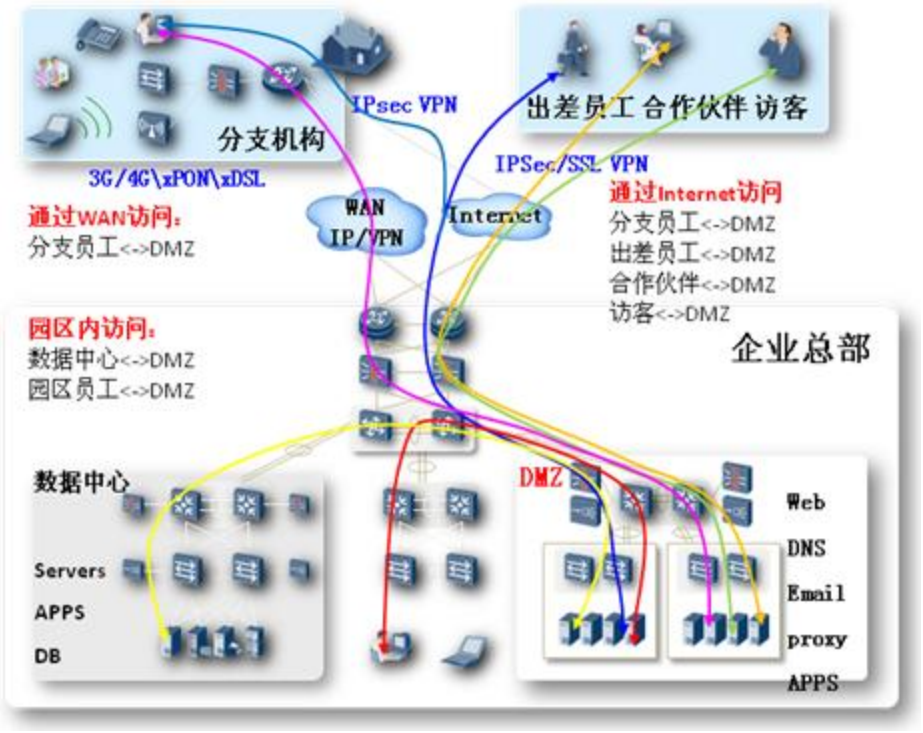
内部网络属于较安全的区域，是绿色区域，风险比较低。主要的安全风险来自内部网络自身的用户（如用户未经授权的存取）。在接入设备中，根据实际需求控制不同分支之间的数据互通的访问控制。

数据中心出口交换机处部署防火墙设备进行安全检查和权限控制；接入层交换机处部署负载均衡器实现服务器资源的有效利用；数据中心出口交换机采用双链路接入园区核心层交换机，实现高可靠性。数据中心内部的设计请参见《数据中心解决方案技术建议书》

2.4 DMZ 区规划

DMZ 区是部署对外业务和服务的区域，狭义的 DMZ 仅对互联网用户提供服务。广义的 DMZ 区还对内部用户或合作伙伴提供服务。

图2-13 DMZ 区规划图



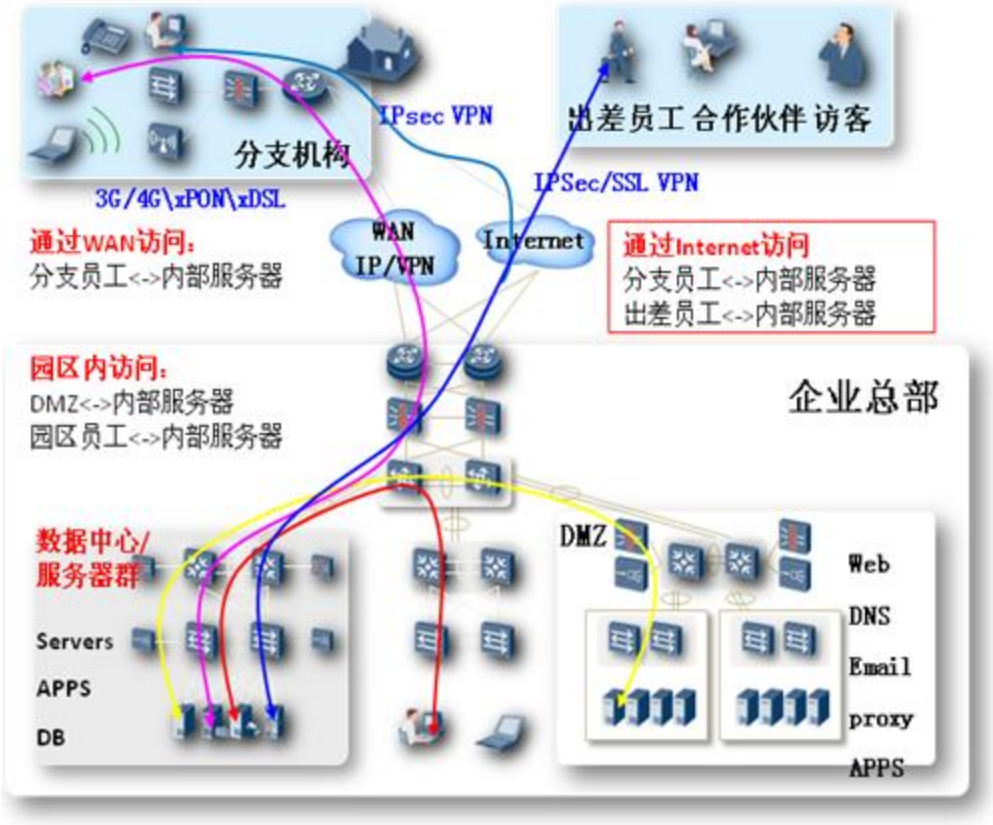
设置 DMZ 区是出于安全性和业务便利性的考虑。DMZ 区放置对外服务的 Web、FTP、Email 服务器，也放置方便内部用户访问 Internet 的 Proxy、DNS 服务器等。外部用户可以访问 DMZ 区的 Web、FTP 等服务，但不能访问到内部的服务。内部用户可以访问 DMZ 区也可以访问内部的服务。

2.5 内部服务区规划

内部服务器区用于放置为企业内部提供服务的服务器。

对外服务所需的 APP 和 DB 服务器，建议放在 DMZ 区，规模达到一定程度需要建设专门的数据中心。

图2-14 内部服务器规划图



由于内部用户能够造成更大的安全威胁，所以内部服务器采取“未经明确允许的就是被禁止的”及“最小授权”的严格安全策略。内部服务器区安全部署重点关注内部子分区的隔离，按照企业组织、密级、业务进行子分区划分。各子分区共用的设备，不同部门或业务采用虚拟技术隔离，如 VLAN、VPN 实例；子分区分开使用的设备，网络管理、系统管理在物理位置上分开。

通过 NAT 技术实现公网和私网的转换，通过 IPSec、SSL VPN、GRE over IPSec 等技术实现安全访问。

3 园区网络技术方案

3.1 VLAN 规划

3.1.1 VLAN 概述

VLAN 是将 LAN 内的设备逻辑地而不是物理地划分为一个个网段，从而实现在一个 LAN 内隔离广播域的技术。当网络规模越来越庞大时，局部网络出现的故障会影响到整个网络，VLAN 的出现可以将网络故障限制在 VLAN 范围内，增强了网络的健壮性。

3.1.2 VLAN 功能划分

用户 VLAN

用户 VLAN 即普通 VLAN，也就是我们日常所说的 VLAN，是用来对不同端口进行隔离的一种手段。VLAN 通常根据业务需要进行规划，需要隔离的端口配置不同的 VLAN，需要防止广播域过大的地方配置 VLAN 用于减小广播域。

Voice VLAN

Voice VLAN 是为用户的语音数据流划分的 VLAN，用户通过创建 Voice VLAN 并将连接语音设备的端口加入 Voice VLAN，可以使语音数据集中在 Voice VLAN 中进行传输，便于对语音流进行有针对性的 QoS 配置，提高语音流量的传输优先级，保证通话质量。

Guest VLAN

网络中用户在通过 802.1x 等认证之前接入设备会把该端口加入到一个特定的 VLAN（即 Guest VLAN），用户访问该 VLAN 内的资源不需要认证，只能访问有限的网络资源。用户从处于 Guest VLAN 的服务器上可以获取 802.1x 客户端软件，升级客户端或执行其他应用升级程序（例如：防病毒软件、操作系统补丁程序等）。认证成功后，端口离开 Guest VLAN 加入用户 VLAN，用户可以访问其特定的网络资源。

Multicast VLAN

Multicast VLAN 即组播 VLAN，组播交换机运行组播协议时需要组播 VLAN 来承载组播流。组播 VLAN 主要是用来解决当客户端处于不同 VLAN 中时，上行的组播路由器必须在每个用户 VLAN 复制一份组播流到接入组播交换机的问题。

3.1.3 VLAN 规划原则

一个二层网络规划的基本原则：

- 区分业务 VLAN、管理 VLAN 和互联 VLAN
- 按照业务区域划分不同的 VLAN
- 同一业务区域按照具体的业务类型（如：Web、APP、DB）划分不同的 VLAN
- VLAN 需连续分配，以保证 VLAN 资源合理利用
- 预留一定数目 VLAN 方便后续扩展

3.1.4 VLAN 规划建议

VLAN 根据多种原则组合划分。

- 按照逻辑区域划分 VLAN 范围：
  例如：
  - 核心网络区：100～199
  - 服务器区：200～999，预留 1000～1999
  - 接入网络：2000～3499
  - 业务网络：3500～3999
- 按照地理区域划分 VLAN 范围
  例如：
  - 接入网络 A 的地理区域使用 2000~2199
  - 接入网络 B 的地理区域使用 2200~2399
- 按照人员结构划分 VLAN 范围
  例如：
  - 接入网络 A 地理区域 A 部门使用 2000~2009
  - 接入网络 A 地理区域 B 部门使用 2010~2019
- 按照业务功能划分 VLAN 范围
  例如：
  - Web 服务器区域：200～299
  - APP 服务器区域：300～399
  - DB 服务器区域：400～499

3.2 IP 规划

考虑到后期扩展性，在园区 IP 地址规划时主要以易管理为主要目标。园区网中的 DMZ 区或 Internet 互联区有少量设备使用公网 IP，园区内部使用的则是私网 IP。

IP 地址是动态 IP 或静态 IP 的选取原则如下：

- 原则上服务器，特殊终端设备（打卡机，打印服务器，IP 视频监控设备等）和生产设备建议采用静态 IP。

- 办公用设备建议使用 DHCP 动态获取，如办公用 PC、IP 电话等。

3.2.1 IP 地址规划原则

IP 地址规划的原则

- 唯一性

  一个 IP 网络中不能有两个主机采用相同的 IP 地址。即使使用了支持地址重叠的 MPLS/VPN 技术，也尽量不要规划为相同的地址。

- 连续性

  连续地址在层次结构网络中易于进行路径叠合，大大缩减路由表，提高路由算法的效率。

- 扩展性

  地址分配在每一层次上都要留有余量，在网络规模扩展时能保证地址叠合所需的连续性。

- 实意性

  “望址生意”，好的 IP 地址规划使每个地址具有实际含义，看到一个地址就可以大致判断出该地址所属的设备。

园区 IP 地址基本分类

- Loopback 地址

  为了方便管理，会为每一台路由器创建一个 Loopback 接口，并在该接口上单独指定一个 IP 地址作为管理地址。

  Loopback 地址务必使用 32 位掩码的地址。最后一位是奇数的表示路由器，是偶数的表示交换机，越是核心的设备，Loopback 地址越小。

- 互联地址

  互联地址是指两台网络设备相互连接的接口所需要的地址，互联地址务必使用 30 位掩码的地址。核心设备使用较小的一个地址，互联地址通常要聚合后发布，在规划时要充分考虑使用连续的可聚合地址。

- 业务地址

  业务地址是连接在以太网上的各种服务器、主机所使用的地址以及网关的地址，业务地址规划时所有的网关地址统一使用相同的末位数字，如：.254 都是表示网关。

- 园区网内部的 IP 地址

  建议使用私网 IP 地址，在边缘网络通过 NAT 转换成公网地址后接入公网。

- 汇聚交换机下接入的网段可能有很多，在规划的时候需要考虑路由是可以聚合的，这样可以减少核心网络的路由数目。

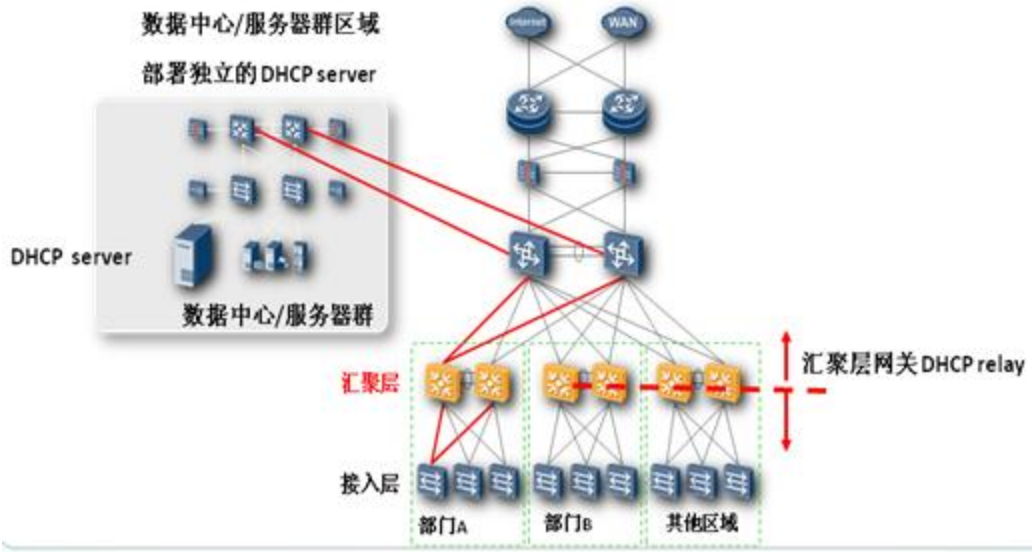
3.2.2 DHCP 规划

园区网中办公网络建议使用 DHCP，每个 DHCP 网段应保留部分静态 IP 供服务器等设备使用。

DHCP 园区部署基本架构

- 在园区数据中心或服务器区部署独立的 DHCP Server。
- 在汇聚层网关部署 DHCP Relay 指向 DHCP Server 统一分配地址。
- DHCP 园区内一般通过 VLAN 分配地址，如有特殊要求，在接入交换机部属 Option82，由接入交换机提供的 Option82 信息分配地址。

图3-1 DHCP 园区部署基本架构



DHCP 部署基本原则

- 固定 IP 地址段和动态分配 IP 地址段保持连续。
- 按照业务区域进行 DHCP 地址的划分，便于统一管理及问题定位。
- DHCP 需要跨网段获得 IP 地址时，启动 DHCP Relay 功能。
- 启动 DHCP 安全功能，禁止非法 DHCP Server 的架设和非法用户的接入。

3.2.3 DNS 规划

DNS 服务器的角色划分

- Master 服务器：主服务器

  作为 DNS 的管理服务器，可以增加、删除、修改域名，修改的信息可以同步到 Slave 服务器，一般部署 1 台。

- Slave 服务器：从服务器

  从 Master 服务器获取域名信息，采用多台服务器形成集群的方式，统一对外提供 DNS 服务，一般采用基于硬件的负载均衡器提供服务器集群的功能。一般部署 2 台从服务器。

- Cache 服务器：缓存服务器

  用于缓存内部用户的 DNS 请求结果，加快后续的访问。一般部署在 Slave 服务器上。

DNS 服务器的 IP 地址

- Master 服务器：采用企业内网地址。
- Slave 服务器：分配企业私网地址，并在负载均衡器上分配一个虚拟的企业内网地址。

Internet 域名地址有两种方案：

- 一种是在防火墙上做 NAT 映射，把 Slave 服务器的虚拟地址映射为一个公网 IP 地址，用于外部 Internet 用户的访问。
- 另一种是在链路负载均衡设备上通过智能 DNS 为外部 Internet 用户提供服务。

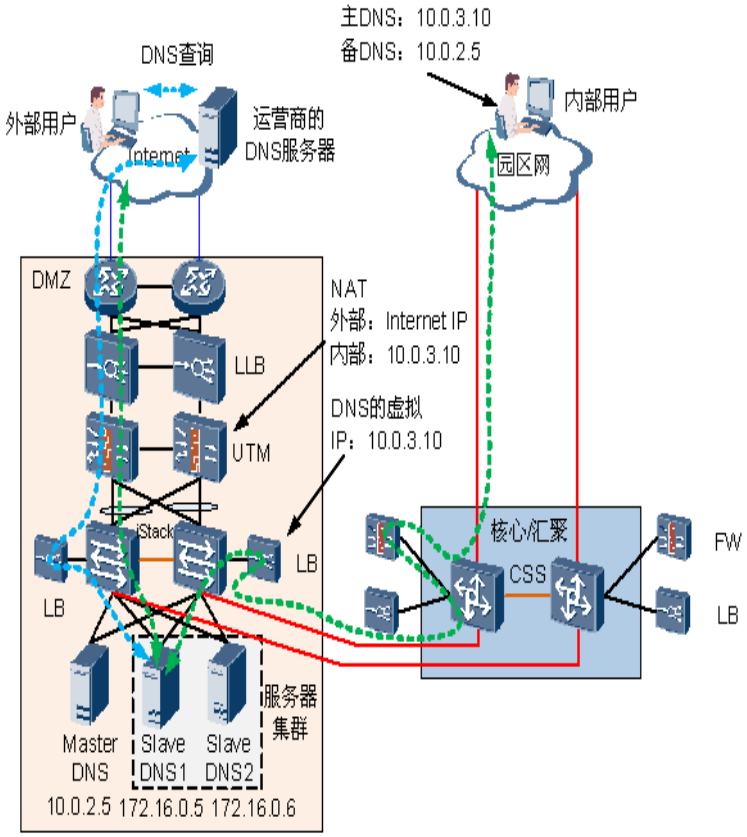
DNS 可靠性设计

众多内部用户发送 DNS 请求，被均匀分担到 Slave DNS1 和 DNS2。当 Slave DNS1 服务器故障后，所有的 DNS 请求被分发给 Slave DNS2。最终 DNS 服务器必须与外部 DNS 通讯。

Master 服务器，建议放置在 DMZ 区域，并在同区内部建立 Slave DNS 服务器。如只对内提供服务的 DNS 服务器，可以作为二级的 DNS 服务器，放入其他非 DMZ 区域。

当所有的 Slave DNS 都故障后，用户发送的 DNS 请求无响应。用户就切换到备 DNS，由 Master DNS 处理所有的请求。

图3-2 园区 DNS 规划

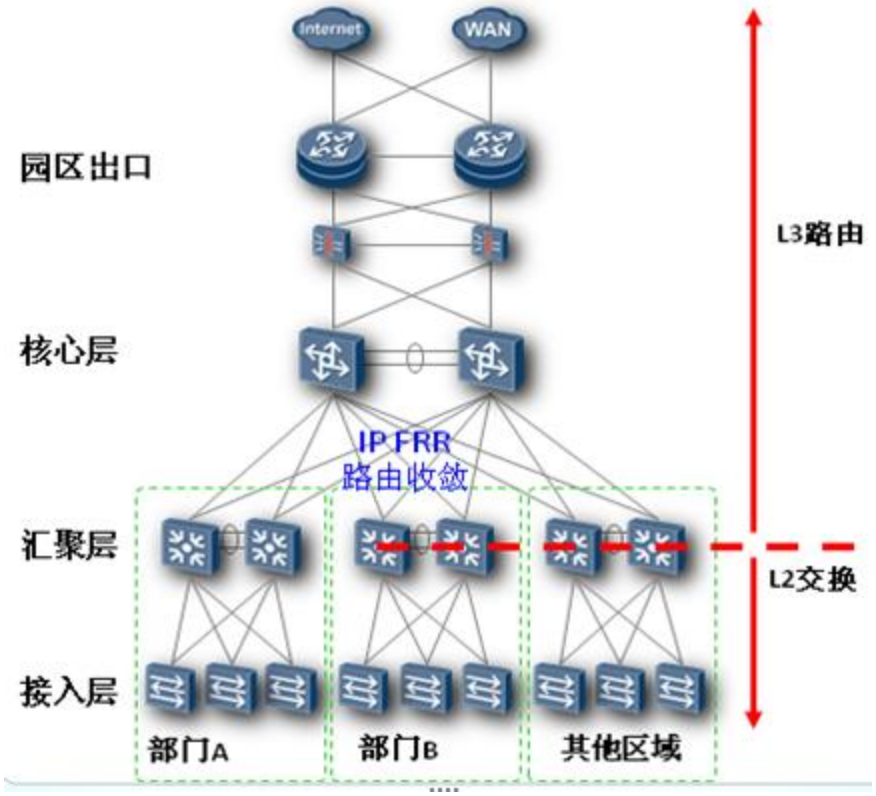


3.3 二层设计

3.3.1 概述

建议采用如图 3-3 所示的网络分层，汇聚层作为网关，接入层做透传转发。这种设计方法下，接入层作为二层转发，需要部署破环协议。

图3-3 二层设计组网图



3.3.2 STP

STP 体系目前有三种协议可用，他们是 STP（IEEE802.1D）、RSTP(IEEE802.1w)和 MSTP(IEEE802.1s)。

在一些老的设备上默认启用 STP。由于 STP 的收敛速度慢，所以在一些后来生产的设备上，都默认启用 RSTP 或者 MSTP。

具体选用哪一种生成树协议，还要看网络的具体拓扑情况。

首先要明确什么时候需要部署 STP，运行 STP 的首要条件就是网络中存在冗余链路。接下来，才要考虑选用哪种 STP 协议。针对存在的三种 STP 协议，需要进行如下考虑：

- 一些比较老的交换机可能不支持 RSTP 或者 MSTP，在有这些设备存在的网络中，就现实情况而言，还是应该启用 STP 协议。如果资金允许，可以将不支持 RSTP 或 MSTP 的设备换掉，因为采用 RSTP、MSTP 可以提升网络的性能。

- 在设备都支持RSTP协议的情况下，当网络中仅存在一个VLAN时，建议采用RSTP，这样可以充分发挥 RSTP 的优势，加速网络的收敛。另外，如果网络中存在多个 VLAN，并且各个 VLAN 在拓扑上保持一致，也就是说在 trunk 链路上各个 VLAN 的配置相同，也建议使用 RSTP。
- 基于上一条描述的条件，当网络中存在多个 VLAN，但是他们在 trunk 链路上的配置并不一致时，就要采用 MSTP 启用多个生成树实例。

网络部署 STP 时，给出下列建议：

- 根桥和备份根桥的选择

  根桥的选择合适与否直接影响着网络的性能。在一个合理根桥设置的网络中，会加快网络的收敛，数据报文会经过更短的路径到达目的地。基于此目的，应本着两点原则进行根桥的选择：

  - 根桥和备份根桥应进行手动选择，不应该让网络自动选择。手动选择可以达到网络的最优化。
  - 优选二层网络的核心设备作为根桥或备份根桥。这里的核心包括处理性能上的优异和网络拓扑位置上的核心层。数据网络的核心通常意味着距离服务器或者路由器更近甚至直连，把根桥放在这个位置就意味着缩短了客户端到服务器或者路由器的平均距离。

  说明

  当设置一台交换机为根桥或者备份根桥之后，用户不能再修改交换机的优先级。并且同一台交换机不能既作为根桥，又作为备份根桥。

- 路径开销的规划

  路径开销（PathCost）是一个端口量，反映了本端口所连接网络的开销。该值越低，表示这个端口所在的链路带宽越大。在一个 STP 网络中，某端口到根桥累计的路径开销就是通过所经过的各个桥上的各端口的路径开销累加而成，这个值叫做根路径开销（RootPathCost）。

  根路径开销的值直接影响着根端口的选择。在一台交换机上所有使能 STP 协议的端口中，根路径开销最小的就会成为根端口。因此，根路径开销的设计也直接影响着数据的转发。

  端口的路径开销也是生成树计算的重要依据，在 MSTP 中，在不同 MSTI 上为同一端口配置不同的路径开销值，可以使不同 VLAN 的流量沿不同的物理链路转发，实现按 VLAN 的负载分担功能。

- MSTP 域和实例的规划

  对于属于同一个域内的所有设备，应遵循以下几条配置原则：

  - 域名必须一致。
  - 域修订等级必须一致。
  - 域内 VLAN 和 MSTI 的映射关系必须一致。
  - 每个 VLAN 只能对应一个 MSTI，即同一 VLAN 的数据只能在一个 MSTI 中传输；而一个 MSTI 可能对应多个 VLAN。
  - 与终端相连的端口建议配置为边缘端口。

3.3.3 RRPP

RRPP（Rapid Ring Protection Protocol）是一个专门应用于以太网环的二层协议，来源于EAPS 协议（RFC3619），该协议提供最快 50 毫秒的保护性能。该协议在 IEEE802.1 中的位置和 STP 相同。RRPP 协议报文采用硬件广播转发，而非 STP 的逐跳处理。

与 STP 协议相比，RRPP 协议有如下特点：

- 拓扑收敛速度快，收敛时间最小可达 50 毫秒。
- 收敛时间与环网上节点数无关，与网络规模无关。

RRPP 部署注意事项

- 在固定的单环和主环/子环拓扑模型上部署。
- 子环要固定连接到主环上，支持 1 级子环。
- 网络完整时，阻断端口是主节点从端口，根据网络拓扑，规划从端口。
- RRPP 环上端口不建议配置风暴抑制功能，避免因为丢弃 RRPPHello 报文导致广播风暴，误操作或者其他异常情况可能导致广播风暴，影响整网业务。
- RRPP 环内新增节点时，必须在新增节点先配置 RRPP 控制 VLAN。如果没有提前配置控制 VLAN，而数据 VLAN 已经打开的情况下，RRPP 会因为 Hello 报文中断导致广播风暴。
- 每个环都必须使用唯一的控制 VLAN，如果主环下挂接大量子环，会占用大量 VLAN，配置前做好网络的 VLAN 规划。

RRPP 的应用场景和注意点

RRPP 协议应用于对保护性能要求较高的简单二层以太网络，支持固定的单环、主环/子环拓扑模型。

在华为公司的二层协议的定位中，RRPP 正被更优秀的 SEP（Smart Ethernet Protection）协议替代。

3.3.4 SEP

SEP 支持各种类型的复杂组网，例如：支持与 STP、RSTP、MSTP、RRPP 协议混合组网，支持任意拓扑且支持拓扑查看。通过查看拓扑可快速找出阻塞端口。当有故障产生，可快速定位故障出现的位置，从而提高了可维护性。SEP 支持多种阻塞端口选择策略，从而灵活地实现了流量负载分担，收敛时间在 50ms 以内。

SEP 协议具有环网协议基本的快速保护性能：

- 拓扑收敛速度快。
- 收敛时间与环网上节点数无关，与网络规模无关。

SEP 的局限性和应用限制

SEP 是我司私有协议，不能和其他公司设备直接对接。

说明

SEP 协议具备较强的混合组网能力，从一定程度上解决了这个问题。

SEP 的应用场景和注意点

SEP 协议应用于对保护性能要求较高的二层以太网络，可以支持复杂拓扑模型，是华为公司目前主推的快速环网保护协议。典型场景包括四种：

图3-4 SEP 单环

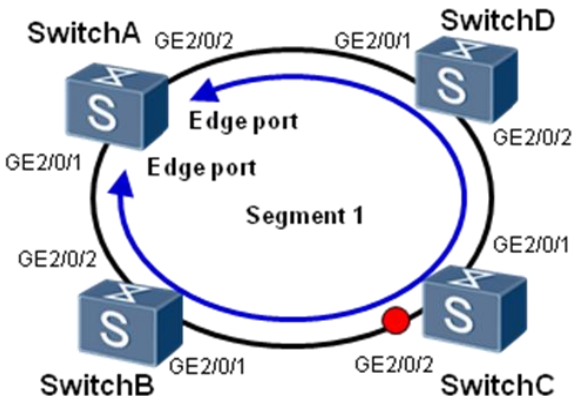


图3-5 SEP 多环

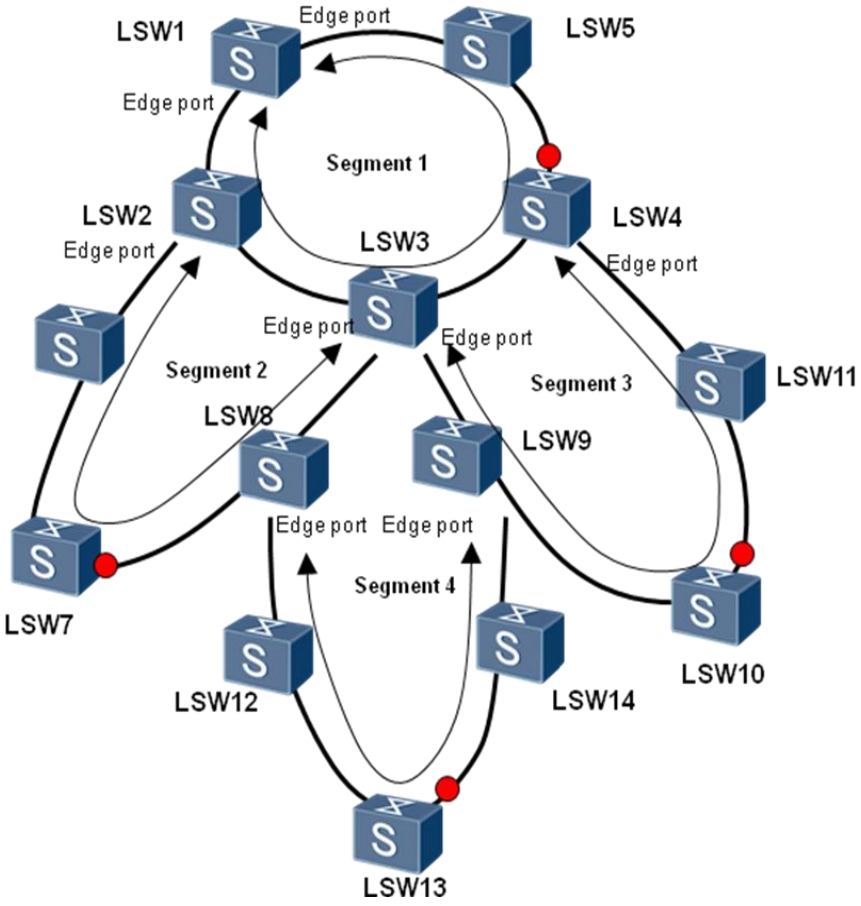


图3-6 SEP 通过普通 edge 端口与 STP 混合组网

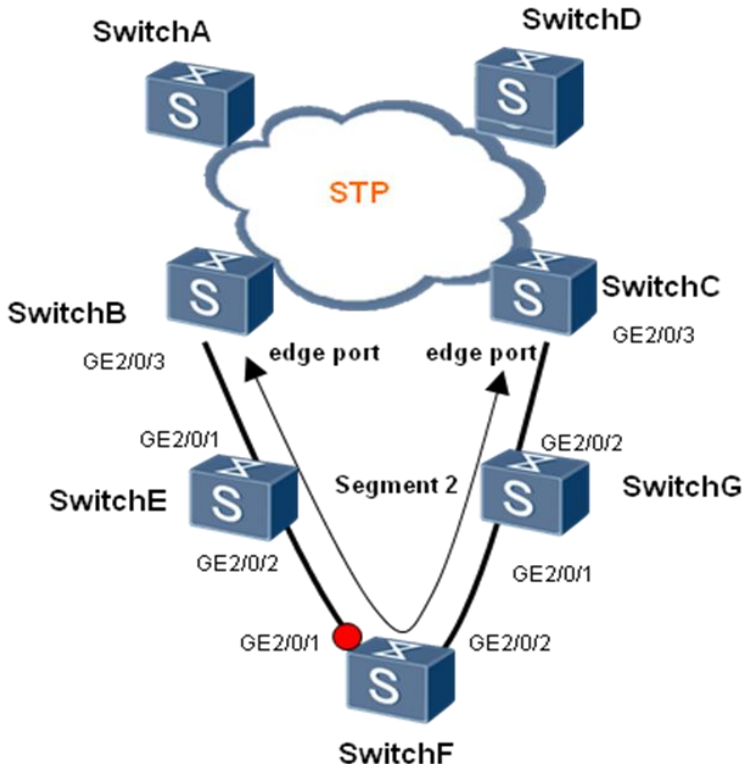
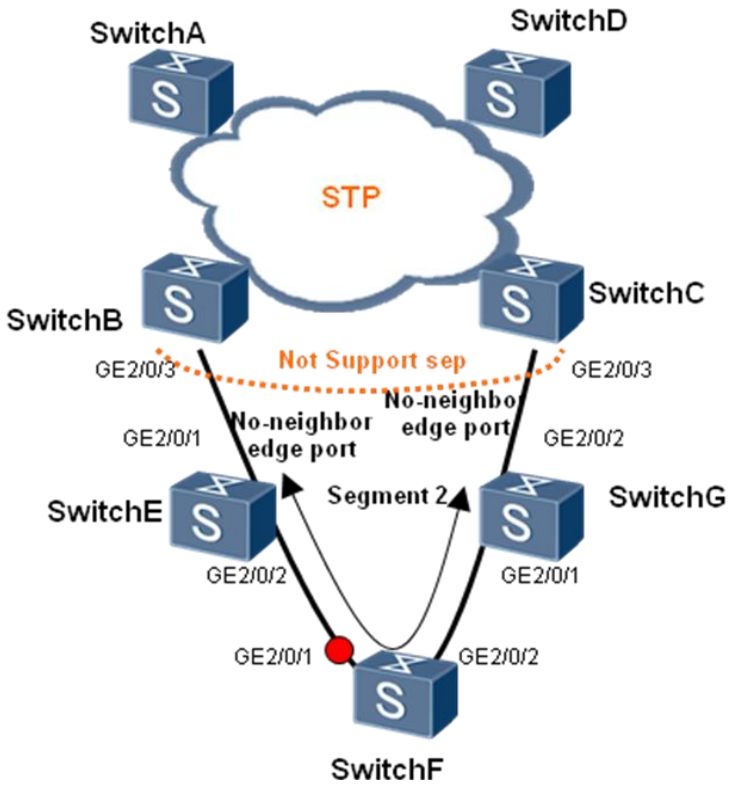


图3-7 SEP 通过 no-neighbor-edge 端口与 STP 混合组网



3.3.5 CSS/iStack

园区网络一般分层部署，大型园区网络分为接入层、汇聚层和核心层。为保证可靠性，部署双上行链路，不可避免链路冗余，需要部署破环协议，随着网络规模的不断扩大，xSTP 协议收敛时间慢，可用性差，由此引出新的解决方案，即 CSS/iStack 技术。

为了提高园区网的可靠性，在接入层推荐采用 iStack（堆叠）技术，即多台交换机堆叠在一起，选举出一台换机做为主交换机，一台交换机为备交换机，剩下的交换机称为从交换机。主交换机是整个堆叠系统中的控制中心。堆叠中每一台交换机都同时具备成为主交换机或者备交换机的能力。

iStack 中多台交换机作为一个整体对外体现为一台逻辑设备，共用一个管理 IP 地址和一个 MAC 地址，且组建方便。堆叠的运维费用低，空间占用小，绿色节能。

核心层采用 CSS（集群）技术，汇聚采用 CSS 或 iStack 技术，即将两台交换机通过专用的堆叠电缆连接起来，选出一台为主交换机，一台为备交换机，对外呈现为一台逻辑交换机。

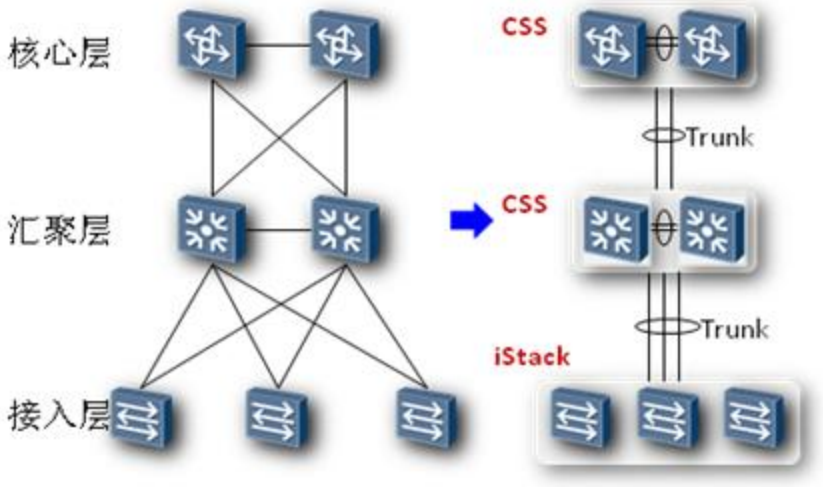
CSS/iStack 技术在网络扩容时，保护已有网络规划不变，扩容方便简单，扩容的同时，将两台物理设备虚拟为一台设备，简化了设备的配置和管理。多台设备间冗余、备份，提高系统的可靠性。

不同网络层级之间建立 Eth-Trunk，支持跨成员端口聚合，消除了 Eth-Trunk 在单台交换机上的单点故障。具有很高的可用性。Eth-trunk 是物理层协议，是将一组物理接口捆绑在一起作为一个逻辑接口来增加带宽的一种方法。通过在两台设备之间建立链路聚合

组，可以提供更高的通讯带宽和更高的可靠性。链路聚合不仅为设备间通信提供了冗余保护，而且不需要对硬件进行升级。Eth-Trunk 的负载分担模式分为手工负载分担模式和静态负载分担模式。

CSS/iStack 技术代替传统的 MSTP+VRRP 组网，克服了网络复杂时 MSTP 收敛时间过长、网络拓扑不稳定的弊端。

图3-8 CSS/iStack 拓扑图



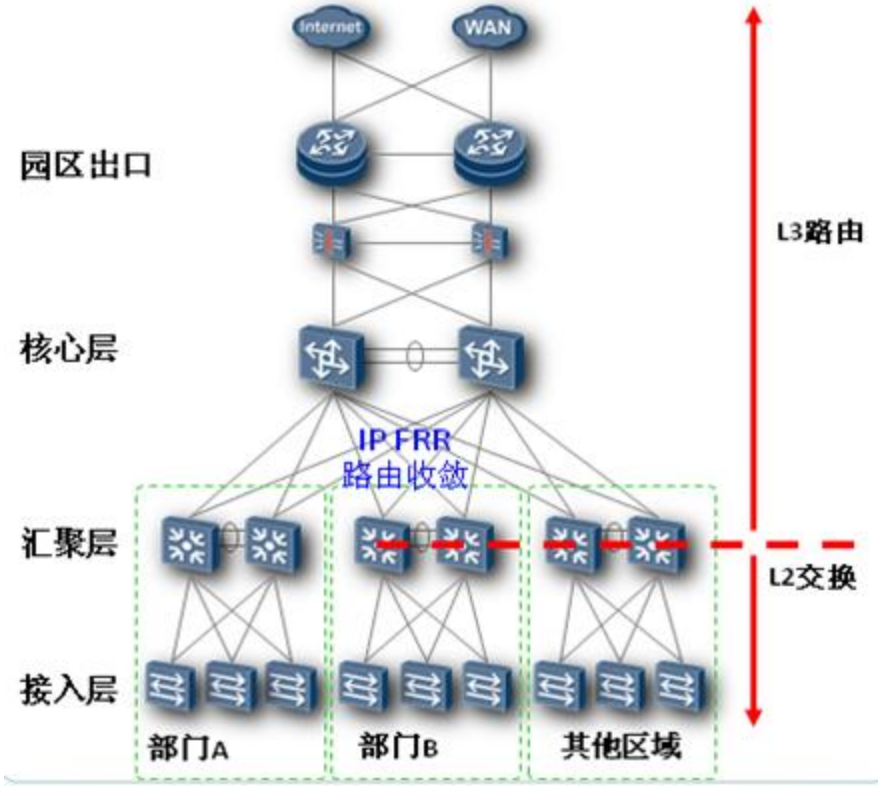
对可靠性要求较高的企业，推荐使用 CSS/iStack 技术，无需部署破环协议，网络拓扑简单，带宽利用率高，网络可靠性高。

3.4 路由设计

3.4.1 路由概述

建议采用汇聚交换机作为路由和交换的分界点。

图3-9 路由交换分界点设计



这种设计方法有如下的优点：

- 路由配置简单

  只需要在 2 台汇聚/核心交换机上配置路由。大量的接入交换机只做二层交换，配置简单。便于采用接入交换机的“自动配置”功能，减少配置维护工作量。

- 扩展性好

  在同一个汇聚/核心交换机下的服务器扩容方便，并且随着业务的变化不需要更改网络的配置，即插即用。

3.4.2 IGP 设计

IGP 协议选择

由于园区网内部可能存在不规则区域，且路由节点不是特别多，建议使用 OSPF 路由协议。每个业务部门区域作为一个单独的 OSPF 区域。

OSPF 规划

- 规划合理的 RouteID

  RouteID 建议采用 Loopback 接口 IP 地址。

- OSPF 核心区域规划

出口路由器和核心交换机作为 OSPF 的 Area0，出口路由器作为 ASBR 和 ABR，核心交换机为 ABR。每个汇聚交换机和核心交换机组网部署为不同的 OSPF Area ID1，2，N。

- OSPF 边缘区域规划

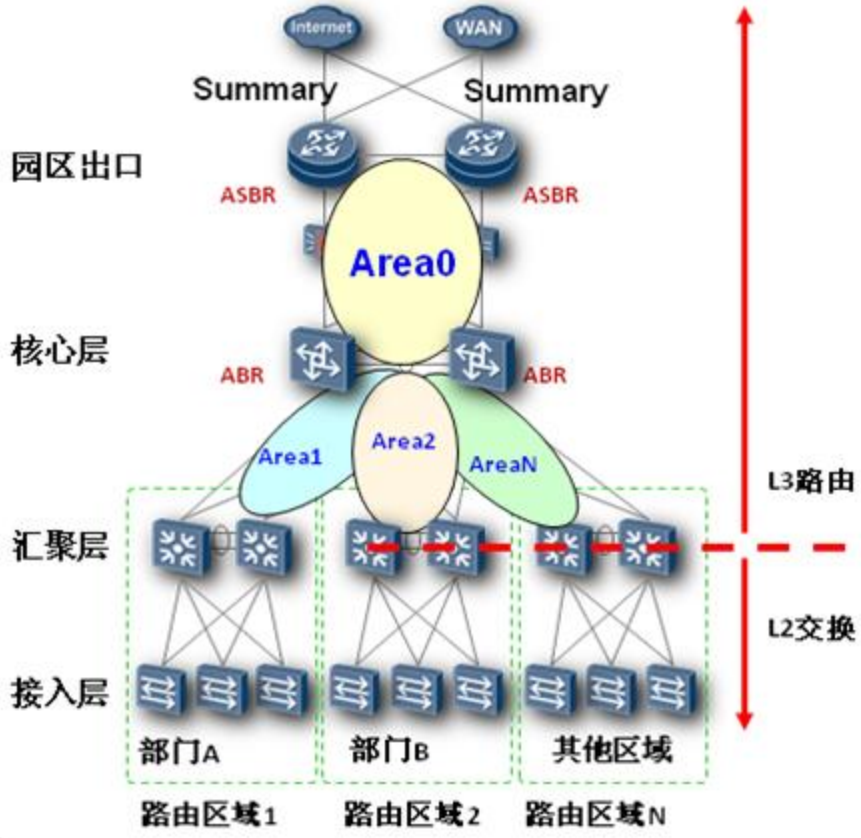
  每个汇聚交换机和核心交换机组网部署为不同的 OSPF Area ID1,2,N，Area1,2,N 使用 OSPFNSSA 区域。与原先的普通的完全 OSPF 区域相比，通过规划减少 LSA 在区域间的传播，减少路由条数；和纯 stub 区域相比部署路由协议更加灵活。另外核心交换机和出口路由器通过区域汇总，限制了区域间传播的 LSA 条目。

  边缘区域使用 NSSA 区域的优势在于：能精简骨干区域路由器的路由表；减少骨干区域内 OSPF 交互的信息量；提高路由表项的稳定性。

一个区域的路由计算和网络调整不会影响其它区域，因故障引起的路由震荡被隔离在区域内部。

如果部门较少，建议只配置 Area0。

图3-10 OSPF 规划图



3.4.3 BGP 设计

园区网中使用 BGP 的场景

- 场景 1

路由数量过于庞大，OSPF 难以胜任时。一般单独一个园区内部路由数目可能不会很多，但是当一个企业分支众多且 IP 规划不十分合理，导致路由条目过多，特别是园区的出口路由器上可建议部署 BGP 进行合理规划引入部分路由。

- 场景 2

  由于业务需要，需要大量的使用路由策略或者是业务分流，使用 OSPF 等协议不擅长，使用 BGP 可以方便的控制路由策略，来分配业务流向。

- 场景 3

  部署 MPLS VPN 技术时，用于复杂的隔离策略等。

园区网使用 BGP 的基本规划

- Routerid 的规划

  BGP 的 routerid 与 OSPF 的 routerid 共用一个，与 Loopback 接口地址相同。

- ASnumber 的规划

  由于企业网中都是私有网络，所以 BGP 使用私有的 AS number。

- IBGP 和 EBGP 的选择

  由于企业网的规模通常都不会很大，通常 IBGP 就可以满足一般的需求了。

BGP 对设备的要求

BGP 协议本身并不消耗很多资源，只有当运行 BGP 的设备需要学习到很多条路由，需要建立很多邻居关系时才会要求设备自身的性能很高。只要规划得当，任何档次的设备（包括接入层设备）都可以运行 BGP 协议。

3.5 组播规划

3.5.1 组播概述

IP 组播技术实现了 IP 网络中点到多点的高效数据传送。相对于数据单播传送，组播有效节省网络带宽，降低对网络设备的要求，用户规模可以灵活变化，用户规模的增大不会对网络和服务器造成带宽和性能压力。所以在实时数据传送、多媒体会议、数据拷贝、游戏和仿真等诸多方面都有广泛的应用。

组播在园区网一般用于特殊场景，例如：网上教学、IP 组播视频会议等业务。

3.5.2 组播地址规划

组播组用 D 类 IP 地址（224.0.0.0～239.255.255.255）来标识。按照使用范围划分，组播地址可以划分为三部分。

- 协议保留组播地址

  地址范围：224.0.0.1～224.0.0.255。此地址范围被 IANA 预留，一般供网络协议使用。该范围内的地址属于局部范畴，此地址的组播报文不能被转发。

- 用户组播地址

地址范围：224.0.1.0～238.255.255.255，此地址范围也称为公用组播地址，在全网范围内有效，可以用于 Internet 上。

- 本地管理组地址

  地址范围：239.0.0.0～239.255.255.255，此地址范围也称为私有组播地址，主要用于测试或供内部网络在内部使用，这个地址的组播不能上公网，类似于单播协议使用的私网地址。

园区内部部署的组播业务只是供本园区内部使用，建议采用本地管理组地址作为组播地址。

3.5.3 组播路由选择

根据协议的作用范围，组播协议分为主机-路由器之间的协议（即组播成员关系管理协议）和路由器-路由器之间协议（即组播路由协议）。

- 组成员关系管理协议包括 IGMP（互连网组管理协议，目前存在 V1、V2、V3 三个版本）；
- 组播路由协议又分为域内组播路由协议和域间组播路由协议两类。

  域内组播路由协议包括：PIM-SM、PIM-DM、DVMRP 等协议；域间组播路由协议包括 MBGP、MSDP 等协议。同时为了有效抑制组播数据在二层网络中的扩散，引入了 IGMP Snooping 等二层组播协议。

园区网络的路由属于域内路由，所以园区网络部署的组播业务不涉及跨域问题。

园区网络域内组播路由推荐使用 PIM 组播路由协议。PIM 不依赖于某一特定单播路由协议，为 IP 组播提供路由信息的可以是静态路由、RIP、OSPF、IS-IS、BGP 等任何一种单播路由协议。组播路由和单播路由协议无关，只要通过单播路由协议能够产生相应组播路由表项即可。与其它组播协议相比，PIM 开销更小，组播效率更高。PIM 定义了两种模式：

- 密集模式（Dense-Mode）

  PIM-DM 密集模式协议，采用了"扩散/剪枝"机制。同时，假定带宽不受限制，每个路由器都想接收组播数据包。PIM-DM 采用反向路径转发 RPF 动态建立最短路径树 SPT。

  该模式适合于组播组成员相对比较密集、组播源和接受者比较靠近、组播数据流比较大且比较稳定、规模较小的网络。

- 稀疏模式（Sparse-Mode）

  PIM-SM 与 PIM-DM 的根本差别在于 PIM-SM 是基于显式加入模型，即接收者向集合点 RP（RendezvousPoint）发送加入消息，而路由器只在已加入某个组播组输出接口上转发那个组播组的数据包。

  PIM-SM 采用共享树进行组播数据包的转发。每一个组有一个集合点 RP，组播源沿最短路径向 RP 发送数据，再由 RP 沿最短路径将数据发送到各个接收端。PIM-SM 主要优势之一是它不局限于通过共享树接收组播信息，还提供从共享树向 SPT 转换的机制。从协议的设计优劣情况比较，PIM-SM 优于 PIM-DM。

  该模式适用于组播组成员分布相对分散、范围较广、视频源多、规模较大的网络。

IGMP 组播成员管理机制是针对第三层设计的。在第三层，路由器可以对组播报文的转发进行控制。但是在很多情况下，组播报文要不可避免地经过一些二层交换设备，如果

不对二层设备进行相应的配置，则组播报文就会转发给二层交换设备的所有接口，这显然会浪费大量的系统资源，IGMP Snooping 可以很好解决这个问题。

IGMP Snooping 运行于二层交换机，是一种二层组播协议，通过侦听上层路由器和用户主机之间发送的组播协议报文来建立二层转发表项，维护组播报文的出端口信息，从而管理和控制组播数据报文的转发。

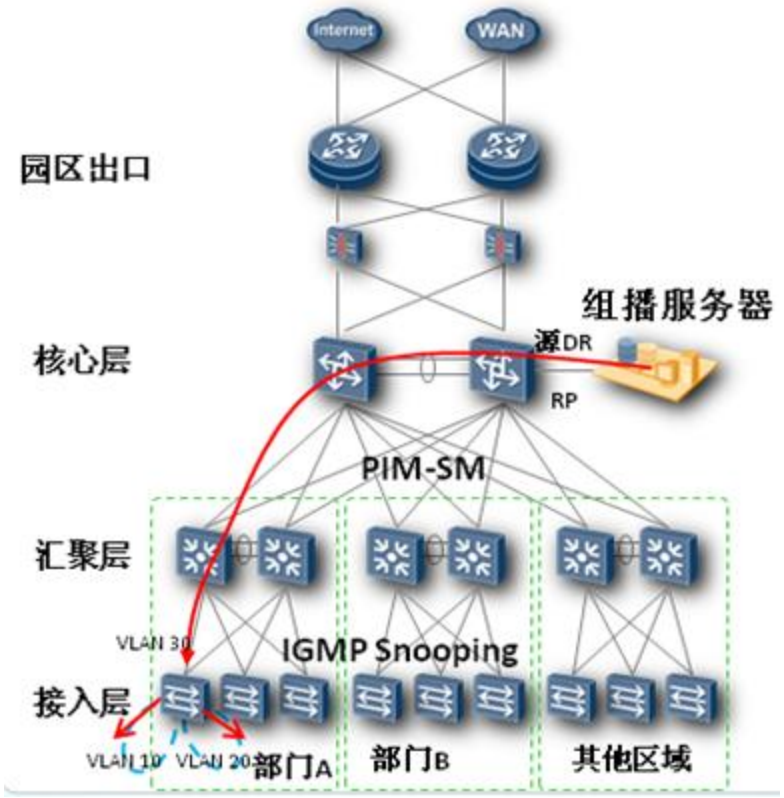
在园区网络中，建议采用采用 PIM-SM+IGMP Snooping 来实现组播业务开展。汇聚交换机到组播源采用 PIM-SM 协议；接入交换机通过 IGMP Snooping+组播 VLAN，实现跨 VLAN 的组播；终端上部署 IGMP。

组播 VLAN 可以满足跨 VLAN 复制的需求，不同 VLAN 的用户分别进行同一组播源点播时，可以在交换机上配置组播 VLAN，并将用户 VLAN 加入组播 VLAN，以实现组播数据在不同的 VLAN 内传送，便于对组播源和组播组成员的管理和控制，同时也可以减少带宽浪费。

园区网络比较简单时，一般 RP 设置在和源 DR 所在的核心交换机上；园区网络比较复杂时，选取一台性能较高的路由器作为源 DR。在采用层次化结构组网的园区网络中，视频源建议直接部署接入核心层上，最大程度减少 PIM-SM 协议范围，缩短组播流量路径，减少组播流量对带宽的占用。所以 RP 选择部署在核心层设备上，从网络的可靠性、可用性等方面综合考虑，选用 2 个核心设备为 RP，通过 Anycast RP 技术可实现负载均衡及冗余，MSDP（Multicast Source Discovery Protocol）是实现 Anycast RP 的关键协议，MSDP 容许 RP 共享活动源信息。

在 Anycast RP 环境,两个 RP 在 Loopback 接口配置相同的 IP 地址。Anycast RP Loopback 地址应当是 32 位掩码的主机地址。IP 路由将自动选择最好的 RP。Anycast RP 提供了 IP Multicast 的快速切换（几秒内）及负载均衡。

图3-11 园区网络组播业务部署



3.6 可靠性规划

3.6.1 设备可靠性

设备本身要具有电信级 5 个 9 的可靠性，需要网络设备支持：

- 主控 1:1 备份
- 交换网 1+1/1:1 两种方式
- DC 电源 1+1 备份；AC 电源 1+1/2+2 备份
- 模块化的风扇设计，高端配置支持单风扇失效
- 无源背板，高可靠性
- 独立的设备监控单元，和主控解耦
- 所有模块支持热插拔
- 完善的告警功能
- 设备管理 1:1 备份

单设备是通过部件的冗余设计来保证高可靠性。对于设备本身的节点故障，一般通过网络协议感知故障点后进行动态调整，实现流量的快速切换，提高可靠性，但是切换的时间比较长。华为支持框式交换机的集群 CSS（Cluster Switch System）和盒式交换机的堆

叠 iStack 技术，能够把多台物理设备连接在一起，对外表现为一台逻辑设备，从功能和管理方面，都可以作为一台设备来看待。单节点物理设备的故障，逻辑设备能够快速感知，并快速将流量切换到 UP 状态的链路上，减少丢包时间，具有更高的可靠性。

采用华为 S97 系列交换机 CSS 技术，对园区核心网络，有如下优势：

- 简化管理和配置

  首先，集群后需要管理的设备节点减少一半以上。

  其次，组网变得简洁，不需要配置复杂的协议，包括 STP/SmartLink/VRRP 等。

- 快速的故障收敛

  链路故障收敛时间可以控制在<10ms,大大降低了网络链路/节点的故障对业务的影响。

- 带宽利用率高

  链路采用 Trunk 的方式，带宽利用率可以达到 100%。

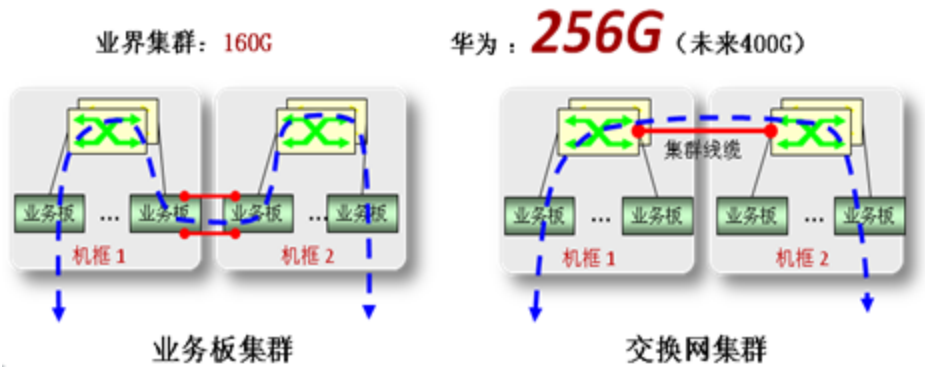
- 扩容方便

  随着业务的增加，当网络需要扩容时，如果采用集群方式，只需要增加新设备即可，不需要更改网络配置。能做到平滑扩容，很好的保护了用户投资。

目前，业界有两种集群的方式。

- 一种是业务板集群（采用业务接口堆叠）
- 一种是交换网集群（采用专用的集群线缆，即堆叠线）。

图3-12 业务板集群和交换网集群



华为的 S97 系列交换机采用交换网集群的方式，通过在主控板上插入堆叠卡，再用堆叠线连接多台设备。相比业务板集群方式，有如下的优势：

- 堆叠带宽高

  交换网集群一般采用专用的接口线，堆叠带宽高。

  S97 系列交换机的堆叠带宽高达 128G(单向)，并且可平滑升级到 320G(单向)。相对于业界的 80G（单向）的互联带宽，具有明显的优势。

- 不占用业务槽位

  S97 系列交换机采用在主控板预留的灵活插卡槽位插入堆叠卡互联的方式，不占用接口槽位。相对于接口堆叠的方式，节省了 1～2 个接口槽位。

- 可靠性高

  S97 系列交换机采用堆叠线连接，实际上是对交换网的延伸。从上图可以看出，业务板堆叠方式需要经过两个堆叠接口板转发，处理复杂度增加；另外，业务板的硬件可靠性也比交换网低。

总体来看，交换网堆叠在软件、硬件及可靠性方面都高于业务板堆叠的方式。

如表 3-1 所示，两种集群方式的比较总结。

表3-1 两种集群方式的比较

集群方式	是否占用业务槽位	集群带宽	转发效率
华为集群	不占用	高：256G（未来 640G）	高：交换网直接互联
业界集群	占用	低：160G	低：需要二次转发

采用华为 S57/37 系列交换机 iStack 技术，对园区接入/汇聚网络，有如下优势：

- 简化管理

  堆叠设备的角色分为 Master 和 Slave。通过对 Master 设备的配置达到管理整个 iStack 堆叠以及堆叠内所有成员设备的效果，而不用物理连接到每台成员设备上分别对它们进行配置和管理。

- 简化网络运行

  iStack 形成的虚拟设备中运行的各种控制协议也是作为单一设备统一运行的，例如路由协议会作为单一设备统一计算。这样省去了设备间大量协议报文的交互，简化了网络运行，缩短了网络动荡时的收敛时间。

- 强大的网络扩展能力

  通过增加成员设备，可以轻松自如的扩展堆叠系统的端口数、带宽和处理能力。

- 高可靠性

  堆叠的高可靠性体现在多个方面，比如：成员设备之间堆叠物理端口支持聚合功能，堆叠系统和上、下层设备之间的物理连接也支持聚合功能，这样通过多链路备份提高了堆叠系统的可靠性；堆叠系统由多台成员设备组成，Master 设备负责堆叠的运行、管理和维护，Slave 设备在作为备份的同时也可以处理业务，一旦 Master 设备故障，系统会迅速自动选举新的 Master，以保证通过堆叠的业务不中断，从而实现了设备级的 1:N 备份。

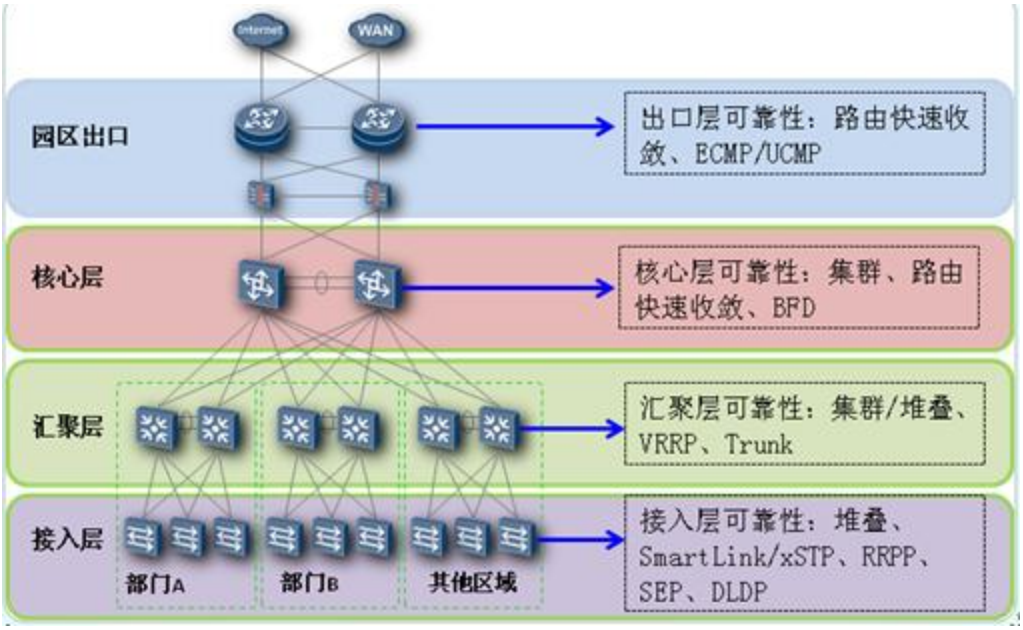
- 高性能

  由于 iStack 设备是由多个支持 iStack 特性的单机设备堆叠而成的，iStack 设备的交换容量和端口数量就是 iStack 内部所有单机设备交换容量和端口数量的总和。因此，iStack 技术能够通过多个单机设备的堆叠，轻易的将设备的交换能力、用户端口的密度扩大数倍，从而大幅度提高了设备的性能。

3.6.2 网络可靠性

园区网络高可靠性设计方案如图 3-13 所示。

图3-13 园区网络可靠性设计方案



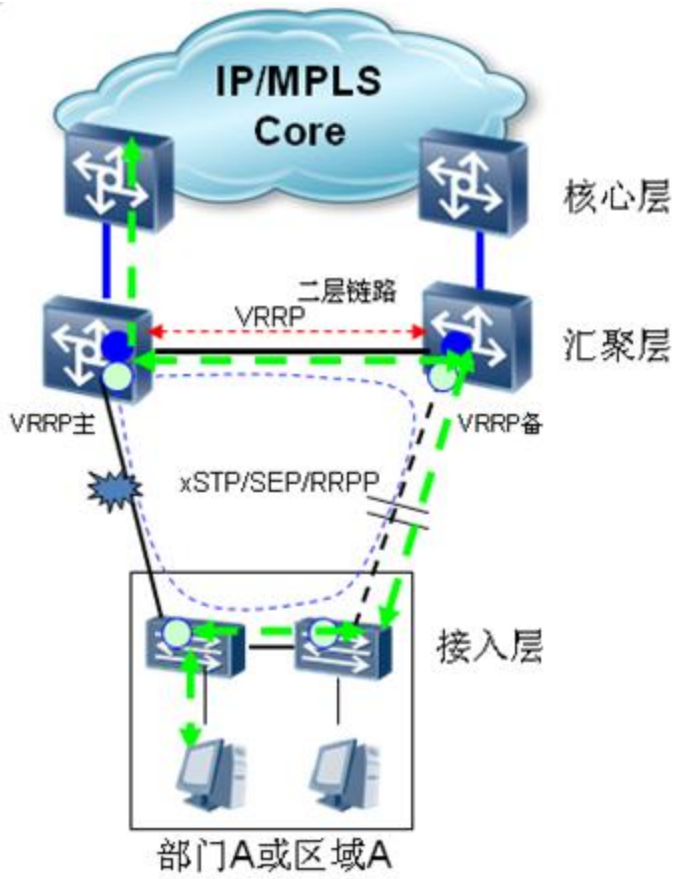
典型园区网络架构为三层网络结构：接入层、汇聚层、核心层。接入交换机为二层交换机，汇聚交换机作为用户网关。可靠性的设计也应该根据层次来设计。

接入层网络是二层网络，接入交换机与汇聚交换机之间通过 SmartLink/STP/RSTP/MSTP/RRPP/SEP 解决二层网络环路问题，同时保证网络可靠性。汇聚交换机之间通过 VRRP（BFD For VRRP）协议确定用户的主备网关，交换机互联通过 TRUNK 链路，保证链路级可靠性，汇聚交换机与接入交换机之间可通过 DLDP 协议检测光纤单向故障（单通故障）。

典型园区网二层可靠性组网设计方案有：口字型组网、三角型组网、U 字型组网。

- 口字型组网

图3-14 二层可靠性组网-口字型



如图 3-14 所示，接入交换机与汇聚交换机之间是二层网络，汇聚交换机作为用户网关设备，两台汇聚交换机之间通过二层 Trunk 链路互连，多台接入交换机与两台汇聚交换机之间组成口字型二层环网，并且通过部署 STP/RSTP/MSTP/RRPP/SEP 等协议进行二层环网阻断、环网故障检测和保护倒换功能。

两台汇聚交换机运行 VRRP（BFD+VRRP）协议确定主备用户网关，VRRP 报文直接在汇聚交换机直连的 Trunk 链路上收发。

注意

两台汇聚交换机链路需要保证绝对可靠，必须采用 Trunk 链路，包含两条以上物理链路。因为汇聚交换机间链路 Down，两台汇聚交换机 VRRP 状态都为主（VRRP 双主情况产生），此时接入二层环网阻塞在汇聚交换机之间的直连链路上，这样接入用户同时感知两个处于 VRRP 主用状态的网关设备（汇聚交换机），会出现问题。

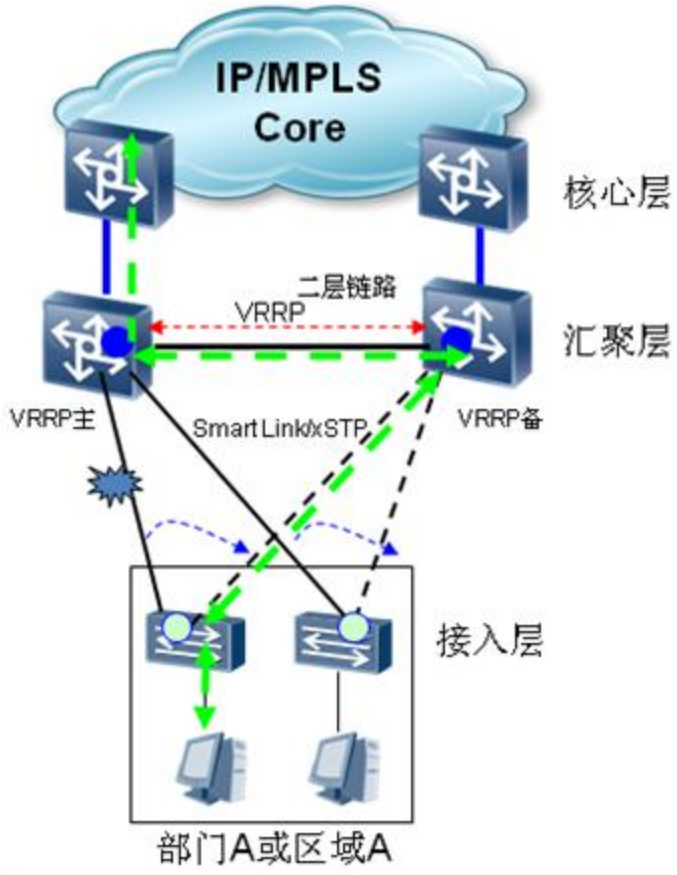
口字型组网方案的优点是：园区网各个楼层接入交换机可以串在一起，与汇聚交换机组成二层环网，汇聚交换机统一为各楼层接入交换机下的用户分配 IP 地址，实现园区不同楼层的用户可以共用同一个 IP 地址网段。

该组网方案的缺点是：接入层网络需要部署较为复杂的二层环网协议，网络配置和维护较为复杂。

口字型组网方案是园区网中非常经典的可靠性设计方案，适合各种规模的园区网应用场景。

- 三角型组网

图3-15 二层可靠性组网-三角型



汇聚交换机作为用户网关设备，两台汇聚交换机之间通过二层链路互连，每台接入交换机上行有两条链路接入到两台汇聚交换机，接入交换机上行两条链路的主备关系由运行的 SmartLink 协议确定。两台汇聚交换机运行 VRRP（BFD+VRRP）协议确定主备用户网关，VRRP 报文直接在汇聚交换机直连链路上收发。

注意

两台汇聚交换机链路需要保证绝对可靠，必须采用 Trunk 链路。三角型组网场景下，多个楼层之间可以共用 VRRP 组，不受汇聚交换机 VRRP 组数量限制，可实现不同楼层间的园区用户可以共享一个 IP 地址网段。

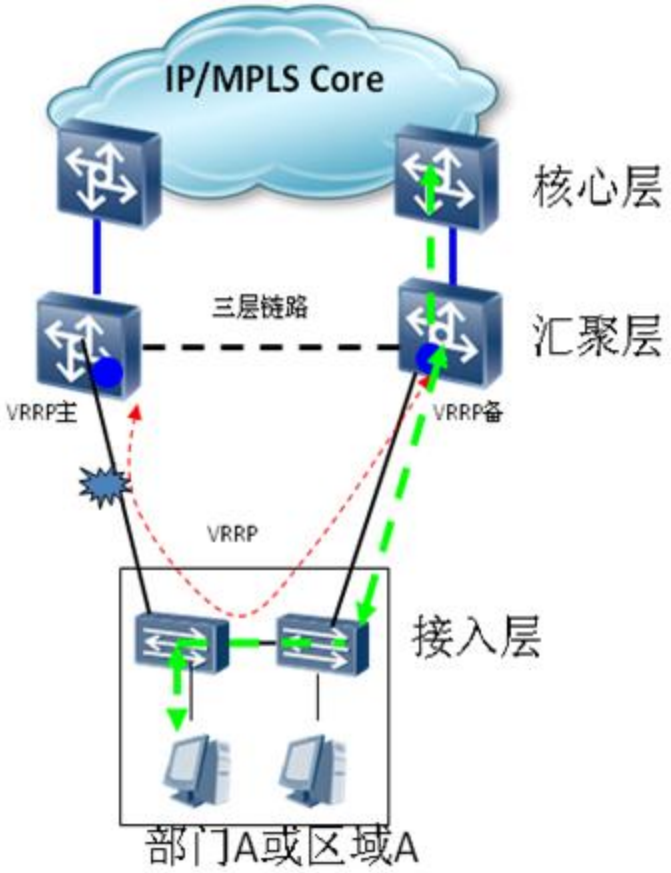
三角型组网中的破环协议也可以使用 xSTP 协议，在配置上会稍微复杂，故障倒换保护速率比 SmartLink 慢。

三角型组网方案的优点是：SmartLink 破环协议部署配置相对复杂的环网保护协议（STP/RSTP/MSTP/RRPP）简单；SmartLink 故障检测和保护倒换速度快（50ms）；支持园区网园区不同楼层的用户可以共用同一个 IP 地址网段。

三角型组网方案的缺点是：每台接入交换机上行需要部署主备两条链路，增加了布线成本，对汇聚交换机的端口密度有较高要求。

- U 字型组网

图3-16 二层可靠性组网-U 字型



U 字型组网中，汇聚交换机之间通过纯三层链路互连，无直连二层链路。汇聚交换机作为园区用户网关，与接入交换机组成二层网络，汇聚交换机的主备通过 VRRP（BFD for VRRP）协议协商，VRRP 协议通过接入交换机转发，每组接入交换机与两台汇聚交换机组成的一个物理 U 型网络。需要启用一组 VRRP，汇聚交换机通过多个物理端口会接入多个二层 U 型网络，这样汇聚交换机间需要运行多个 VRRP 组（每个二层 U 型接入网络运行一个 VRRP 组）。

一般情况下，一个 U 型二层接入网覆盖的是同一个楼层的接入交换机。由于不同 VRRP 组的网关 IP 网段不能相同，因此每个 U 型接入网下的所有园区用户需要独占一个 IP 网段，不同 U 型接入网的用户（不同楼层的园区用户）之间不能共享一个 IP 网段，这是此方案应用的最大缺点。

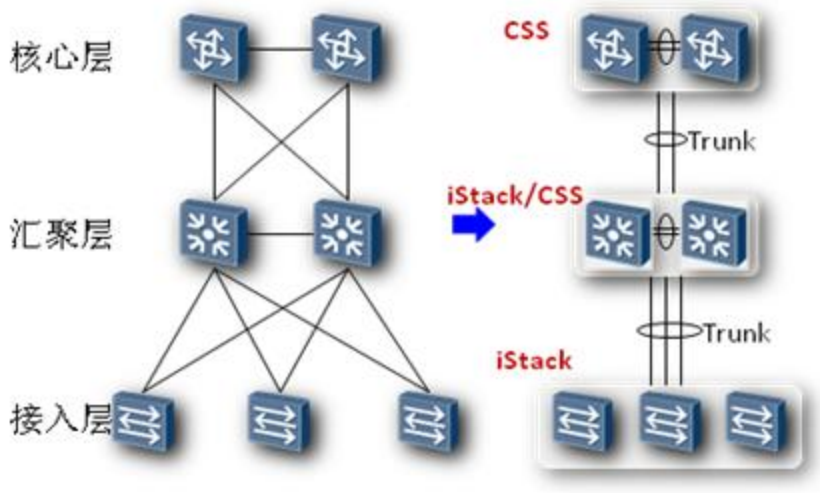
U 字型方案的优点：二层接入网不存在环路，不需要配置相对复杂的环网保护协议（STP/RSTP/MSTP/RRPP）。

从管理维护、收敛时间、部署方面三方面考虑，园区网络二层网络破环协议部署 SmartLink 要优于 xSTP、RRPP、SEP。

园区网可靠性方案设计的目标方案或发展趋势是各层次园区网交换机都进行虚拟化。如图 3-17 所示，通过集群/堆叠技术将两台或多台交换机虚拟成一台交换机。可以提高单节点设备可靠性，一台交换机故障，另外一台交换机自动接管故障设备上的所有业务，可以做到业务无损切换。设备虚拟化通过跨设备的 Trunk 链路，提升链路级可靠性，并且流量可以均匀分布在 Trunk 成员链路上，提高链路带宽利用率，一条或多条链路故障后，流量自动切换到其他正常的链路。

该方案另外一个优点是网络配置和维护简单，园区二层接入网不需要配置复杂的二层环网和保护倒换协议，二层链路故障能直接感知快速切换。三层网络中多个设备间共享路由表，网络故障路由收敛速度快。网络管理和维护难度大大降低，此方案适应面广，扩展性强，是未来园区网的发展趋势。

图3-17 园区网可靠性方案



汇聚层作为接入网关，一般情况下，汇聚层以上设备部署三层网络。在三层网络比较常用的可靠性技术包括：IP FRR、NSF/GR、ECMP/UCMP、BFD。

- IP FRR

  IP FRR（IP Fast Reroute）即 IP 快速重路由。IP FRR 是一种转发快速切换技术，当物理层或链路层检测到故障时无需等待路由收敛，立即开始采取措施，使用一条备份的链路将报文转发出去，从而将链路故障对承载业务的影响降低到最小限度。通常在汇聚层到核心层、核心层到出口路由器之间部署。

  如下图所示，从 A 到 C 之间的路径为主转发路径，当 A 检测到 A 到 C 之间的主路径出现链路故障时，快速切换转发下一跳至 B，启用备份路径，A-B-C 之间的路径为事先建立好的转发路径。

- NSF(GR)

  NSF（None Stop Forwarding）是设备本身可靠性的一种，属于 GR（Graceful Restart）的一种形态。NSF 是指在路由器控制层面故障的过程中，数据转发不间断地正常执行。

通常情况下，路由器故障后，其路由协议层面的邻居会检测到它们之间的邻居关系 Down 掉，然后过段时间再次 UP，这个过程被称之为邻居关系震荡。这种邻居关系的震荡将最终导致路由震荡的出现，使得重启路由器在一段时间内出现路由黑洞或者导致邻居将数据业务从重启路由器处旁路，从而导致网络的可靠性大大降低。NSF 技术的目标就是为了解决上述路由震荡的问题，在设备主控倒换时，转发层面不等待控制平面重新计算路由，先保持现有转发路径不变。NSF 功能通常在所有三层设备上部署。

- ECMP/UCMP

  ECMP（Equal Cost Multiple Path）是解决三层设备之间的转发能力扩展和可靠性问题的协议。根据实际链路情况和需要配置成等价转发路径或者非等价转发路径，实际转发路径通过 HASH 得到，根据需要进行 3 元组、4 元组或者 5 元组 HASH，是解决三层多路径的一种非常好的办法。

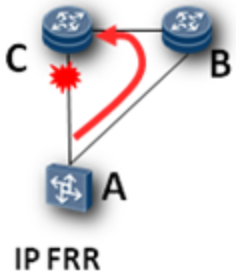
  ECMP 负载分担模式是等价负载分担，而 UCMP（Unequal Cost Multiple Path）则流量会可以根据带宽按比例分担到每条链路上。这样所有链路可根据带宽不同而分担不同比例的流量，使流量转发更合理。ECMP 和 UCMP 主要用于园区出口连接广域网和 Internet 的不同运营商。

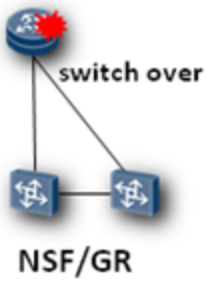
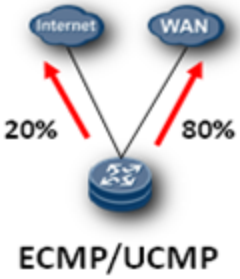
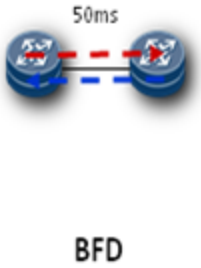
- BFD

  BFD 是一种三层检测机制，对相邻转发引擎之间通道故障提供轻负荷、持续时间短的检测。这些故障包括接口、数据链路，甚至是转发引擎本身。BFD 提供一个单一的机制，它能够用来对任何媒介、任何协议层进行实时地检测，并且检测的时间与开销范围比较宽。

  BFD 故障检测机制与以往的其他“Hello”检测机制相比，具有许多独到的优势。目前的网络路由协议一般采用慢 Hello 机制，在没有硬件帮助下，检测时间会很长（例如：OSPF 需要 2 秒的检测时间，ISIS 需要 1 秒的检测时间）。这对某些应用来说时间太长了，当故障发生时，故障感应时间越长代表着数据丢失量越大。BFD 协议的出现，为上述问题提出了一种解决方案，BFD For 路由，就是将 BFD 和路由协议关联起来，通过 BFD 对链路故障的快速感应进而通知路由协议，从而加快路由协议对于网络拓扑变化的响应。

表3-2 三层可靠性部署建议

三层可靠性保护方式	组网	部署建议
IP FRR		在汇聚层和核心层部署 IP FRR。对主用路径和备用路径可以灵活指定。

三层可靠性保护方式	组网	部署建议
NSF/GR		在核心层和出口路由器上部署 GR 功能，当设备主用主控失效，备用主控接管控制平面，转发平面不受影响。
ECMP/UCMP		部署在出口路由器上，将流量负载均衡到不同的出口链路上。
BFD		在汇聚层配置 BFD For VRRP；在核心层、出口路由器上部署 BFD For OSPF。

3.7 QoS 设计

3.7.1 多业务共存引发 QoS 需求

金融企业园区网络中，除了传统的 WWW、E-Mail、FTP 等数据业务，还承载着视频监控、电视会议、语音电话等业务，这些业务有一个共同特点，即对带宽、延迟、延迟抖动等传输性能有着特殊的需求。比如视频监控、电视会议需要高带宽、低延迟抖动的保证。语音业务虽然不一定要求高带宽，但非常注重时延，在拥塞发生时要求优先获得处理。

服务质量 QoS 是各种存在服务供需关系的场合中普遍存在的概念，它评估服务方对客户的服务需求提供支持的能力，目的就是向用户的业务提供端到端的服务质量保证。一般情况，QoS 度量指标如下：

- 吞吐量（Throughput）：又可称为带宽，表示一定时间内业务流的平均速率。通常通过流量监管（CAR）、流量整形（GTS）实现带宽调度。
- 时延(Latency)：表示业务流穿过网络时需要的平均时间。对于网络中的一个设备来说，一般将不同时延的业务分为几种优先级，通过队列调度保证业务需求。

- 抖动(Jitter)：表示业务流穿过网络的时间的变化，可通过拥塞避免等技术防止流量抖动。
- 丢包率（Drop Ratio）：在网络中传输数据包时丢弃数据包的最高比率。数据包丢失一般是由网络拥塞引起的。

针对带宽、时延、抖动、丢包率等要求，QoS 可以通过优先级映射、流量监管、流量整形、队列调度、拥塞避免等技术提升网络服务质量，满足用户在有限的资源限制情况下，获得多业务部署的最佳体验。

3.7.2 建立部署模型

QoS 部署模型

QoS 部署模型规定了多种 QoS 技术如何组合满足用户网络服务需求，当前主要存在以下两种部署模型：

- Int-Serv 模型

  Int-Serv（Integrated Service）模型是一个综合服务模型，它的特点是在发送报文前要先向网络提出申请，一般通过资源预留协议 RSVP 实现。

  可以提供端到端的 QoS 投递服务是 Int-Serv 的最大优点；其最大缺点是可扩展性不好，通信设备需要为每个资源预留维护一些必要的软状态（SoftState）信息，当网络中的数据流数量很大时，设备的存储和处理能力会遇到很大的压力。

- Diff-Serv 模型

  Diff-Serv（Differentiated Service）模型是一种多服务模型，它通过携带在报文头部的优先级参数（802.1P、DSCP、EXP）来告知网络节点它的 QoS 需求，这样，Diff-Serv 在提供服务时，可以为属于同一需求类别的分组提供同样的服务策略，而无需通过信令协议再去申请资源。

  正是由于拥有“带内”信令和基于流进行服务的特点，在网络部署中，Diff-Serv 具有良好的可扩展性，成为企业园区网络部署的主流方案。

用户业务分类

在对于 Diff Serv 部署，RFC4594 把业务划分为 12 种类型，并规划了报文优先级参数和 PHB 动作，如表 3-3 所示：

表3-3 用户业务分类说明

业务分类	RFC 名称	业务说明	PHB	DSCP	802.1P	EXP
网络控制	Network Control	网络控制平面业务，如 OSPF/BGP/VRRP/EIGRP 等。	CS6	48	6	6
语音业务	VoIP Telephony	VoIP 业务，包括 G.711、G.729 等语音流	EF	46	5	5

业务分类	RFC 名称	业务说明	PHB	DSCP	802.1P	EXP
广播视频	Broadcast Video	广播电视和视频监控业务，特点是丢包敏感，不具备重新发送和流控能力。	CS5	40	5	5
桌面会议	Multimedia Conferencing	桌面多媒体协同应用软件，包括语音和视频的应用，如华为eSpace。	AF41、AF42、AF43	32、36、38	4	4
交互视频	Real-time Interactive	室内部署的交互视频应用，具有语音和视频能力。如视频会议、高清视频等	CS4	32	4	4
视频点播	Multimedia Streaming	VoD 视频点播业务。这类业务允许一定的时延，丢包能够重传，比广播和实时媒体业务更具弹性	AF31、AF32、AF33	26、28、30	3	3
呼叫信令	Signaling	IP 语音和视频业务信令流。如 SIP、H323、MGCP、VMP 等	CS3	24	3	3
事务处理	Low-Latency Data	交互式的重要数据业务，如即时消息、ERP、数据库查询	AF21、AF22、AF23	18、20、22	2	2
网络管理	OAM	网络维护和管理业务。SNMP、SSH、Sys Log	CS2	16	2	2
Bulk 数据	High-Throughput Data	指非交互式“背景”业务，其特点是不需要等待业务响应，不会影响工作效率。如 Email、FTP、文件共享等业务	AF1	10、12、14	1	1
背景流量	Low-Priority Data	与公司业务无关，多是娱乐性的业务。如 BT、eMule、YouTube 等非组织性的内容	CS1	8	0	0
尽力服务	Standard	采用默认优先级 0，大多数业务不进行优先级标记	DF(CS0)	0	0	0

RFC4594 为了提高业务识别效率，对不同类别的业务进行了标准的分类标记，把业务分为 12 种类型，其中网络控制业务的相关 QoS 参数一般由交换机、路由器等设备指定，本文不做过多描述；其他属于用户业务，需要用户自己规划 QoS 参数。

按照业界通行做法，广播视频和呼叫信令业务 PHB 不遵循 RFC 标准，进行对调。即广播视频 RFC4594 规定为 CS3，这里采用 CS5；呼叫信令则相反。

流量带宽模型

对于 12 类业务，从对于服务质量要求的角度，可分为以下四类：

- 实时业务（RealTime）

  包括语音业务、呼叫信令、广播视频、交互视频、桌面会议等五类业务，共同特点是要求对于时延要求很高，如果延迟太长的话，就会引起语音、视频质量下降，影响用户最终体验。该类业务总带宽一般不超过 45%。

- 带宽保证业务（GuaranteedBandwidth）

  包括网络控制、视频点播、网络管理、事务处理业务，总带宽约 24%。该类业务共同特点是属于企业内部基本业务，需要保证一定带宽，对于时延不是很敏感。

- 尽力服务业务（BestEffort）

  也称为标准业务，通常 DSCP/802.1P 标记为 0，总体上应当为尽力服务类别分配足够的带宽，建议预留至少 25%。

- 背景传输业务（Scavenger）

  包括 BULK 数据和背景流量，该类业务需要拥有适度的限制带宽，阻止其占用整个链路。一般带宽分配 5%。

各类业务带宽模型如表 3-4 所示：

表3-4 业务带宽模型

业务分类	PHB	流量比例	QoS 品质
网络控制	CS6	2%	带宽保证
语音业务	EF	10%	实时业务
广播视频	CS5	10%	实时业务
桌面会议	AF41、AF42、AF43	10%	实时业务
交互视频	CS4	13%	实时业务
视频点播	AF31、AF32、AF33	10%	带宽保证
呼叫信令	CS3	2%	实时业务
事务处理	AF21、AF22、AF23	10%	带宽保证
网络管理	CS2	2%	带宽保证
Bulk 数据	AF1	5%	背景传输

业务分类	PHB	流量比例	QoS 品质
背景流量	CS1	1%	背景传输
尽力服务	DF(CS0)	25%	尽力服务

规划队列模型

在 QoS 部署中，对于业务完成分类后，需要将这些业务流引入到队列中，通过队列调度实施 QoS 策略。

当前华为数通设备中，主要存在 4 队列、8 队列两种队列模型。

- 4 队列模型

  该类设备一般属于用户侧接入交换机，设备存在 4 个队列资源，在设备出端口通过 4 个队列实施队列策略。队列调度采用 1 个优先级队列 3 个循环队列方式，即 1P3Q 调度，其中最高队列 Q3 定义为优先级队列，其他三个队列进行 WRR 调度。

- 8 队列模型

  设备存在 8 个队列资源，在设备出端口通过 8 个队列实施队列策略。队列调度采用 1P7Q 方式，其中最高队列 Q7 定义为优先级队列，其他 7 个队列进行 WRR 调度。

队列 1P7Q 调度策略

对于 8 队列的设备，可以按照 1P7Q 模型设计：Q7 指定为优先级队列，其他指定为 WRR（DRR）队列，采取混合调度方式实施 QoS 策略。如表 3-5 所示，其中队列 Q6 作为预留队列，没有使用。

表3-5 1P7Q 调度策略

业务分类	PHB	流量	队列	队列带宽	队列调度	拥塞避免
网络控制	CS6	2%	Q5	100%	10%	WRED/SRED
语音业务	EF	10%	Q7	20%	PQ	WRED/SRED
广播视频	CS5	10%				
桌面会议	AF4	10%	Q4	100%	20%	WRED/SRED
交互视频	CS4	13%				
视频点播	AF3	10%	Q3	100%	15%	WRED/SRED
呼叫信令	CS3	2%				
事务处理	AF2	10%	Q2	100%	20%	WRED/SRED
网络管理	CS2	2%				
Bulk 数据	AF1	5%	Q1	100%	5%	WRED/SRED

业务分类	PHB	流量	队列	队列带宽	队列调度	拥塞避免
背景流量	CS1	1%				
尽力服务	DF	25%	Q0	100%	25%	WRED/SRED

- 带宽分配

  语音业务、广播视频等采用 PQ 保证其优先转发的同时，却增加了数据业务的排队时延，甚至丢包。PQ 所占带宽比例越大，PQ 业务瞬间突发对数据业务的冲击就越大。一般设计 PQ 带宽不能超过端口总带宽的 1/3。

  在 1P7Q 模型中，优先级队列 Q7 带宽上限（PIR）设计为 20%，带宽下限不做限制；其他 WRR（DRR）队列带宽上限不做限制。

- 队列调度

  8 个队列采取混合调度，基于带宽要求，WRR（DRR）队列 Q0～Q6 的权值依次为 25：5：20：15：20：10：5。

- WRED 调度

  8 个队列启用 WRED（SRED）调度，丢弃下限和上限按照 80：100 设置。

队列 1P3Q 调度策略

4 队列的设备主要是接入层设备（如 S27 交换机），可以按照 1P3Q 模型设计：Q3 指定为优先级队列，其他指定为 WRR（DRR）队列，采取混合调度方式实施 QoS 策略，如表 3-6 所示。

表3-6 1P3Q 调度策略

业务分类	PHB	流量	队列	队列带宽	队列调度	拥塞避免
语音业务	EF	10%	Q3	30%	PQ	WRED/SRED
广播视频	CS5	10%				
桌面会议	AF4	10%				
交互视频	CS4	13%				
网络控制	CS6	2%	Q2	100%	50	WRED/SRED
视频点播	AF3	10%				
呼叫信令	CS3	2%				
事务处理	AF2	10%				
网络管理	CS2	2%				
Bulk 数据	AF1	5%	Q1	100%	10	WRED/SRED
背景流量	CS1	1%				

业务分类	PHB	流量	队列	队列带宽	队列调度	拥塞避免
尽力服务	DF（CS0）	25%	Q0	100%	40	WRED/SRED

- 带宽分配

  在 1P3Q 模型中，优先级队列 Q3 带宽上限（PIR）设计为端口带宽 30%，带宽下限不做限制；其他 WRR（DRR）队列带宽上限不做限制。

- 队列调度

  8 个队列采取混合调度，基于带宽要求，WRR（DRR）队列 Q0～Q2 的权值依次为 40：10：50。

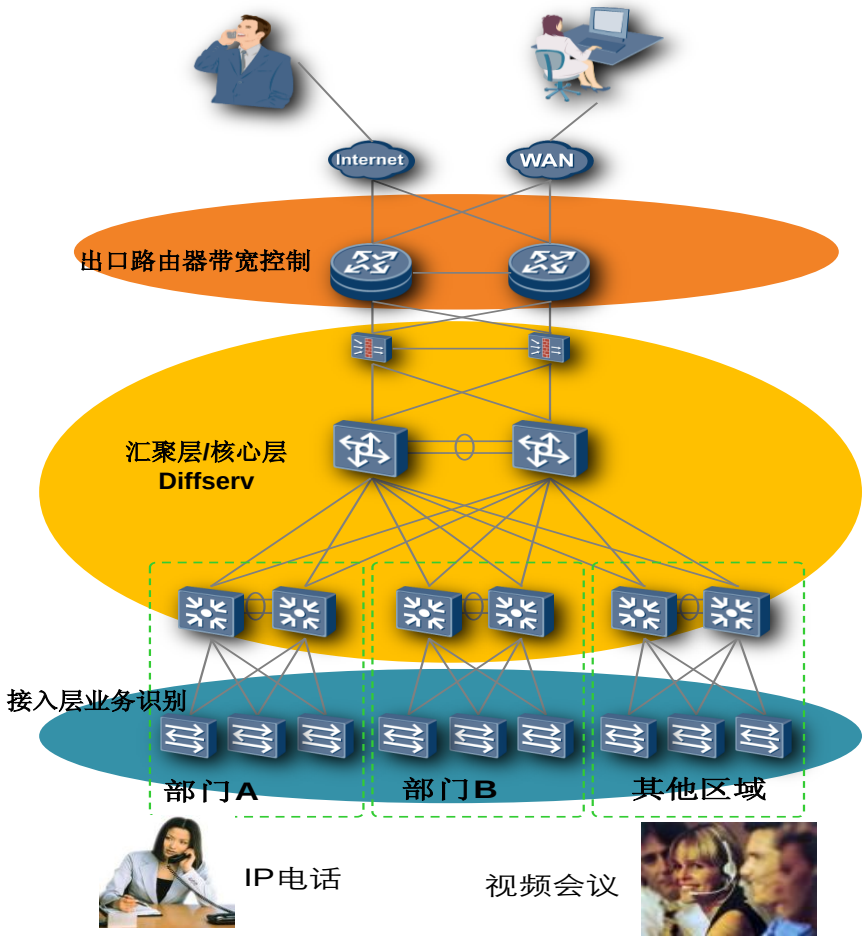
- WRED 调度

  8 个队列启用 WRED（SRED）调度，丢弃下限和上限按照 80：100 设置。

3.7.3 园区网 QoS 部署

园区网部署 QoS 部署图如图 3-18 所示，具体可以按照前面 DiffServ 模型分层实施，主要分为接入层业务识别、汇聚层/核心层 DiffServ 部署、出口路由器带宽控制三个方面。

图3-18 园区网 QoS 部署图



接入层业务识别

接入交换机作为边界交换机，在 UNI（User Network Interface）侧需要担负数据流的识别、分类以及流标记的工作，而在 NNI（Network Node Interface）侧需要担负不同应用数据流的拥塞管理、拥塞避免、流量整形等工作。

在实际部署的时候，接入交换机上不同的端口接入了不同的终端，在接入交换机上可以给这些不同的业务分配不同的优先级，之后，在网络中按这样的优先级进行调度就可以了。

汇聚层/核心层 Diffserv 调度

汇聚层和核心层设备端口信任 DSCP（或者 802.1P），基于接入层标识的 QoS 参数，通过队列调度、流量整形、拥塞避免等方式实施 QoS 策略，保证高优先级业务优先获得调度。

出口路由器带宽控制

对于出口路由器，同样作为 DiffServ 域，信任设备标识的 DSCP/802.1P 参数，实施 QoS 策略。需要说明的是，在路由器的 WAN 口上，由于受限于出口带宽，相关 WAN 口带宽参数设置需要考虑差异性。

3.8 安全设计

3.8.1 安全概述

随着企业网络的应用和发展，企业生产和经营活动对于网络的依赖性不断增强。但病毒、木马、间谍软件、网络攻击等各种信息安全威胁也在不断增加。统计表明，网络安全已经超过对网络可靠性、交换能力和服务质量的需求，成为企业用户最关心的问题，网络安全基础设施也日渐成为企业网建设的重点。

在传统的园区网络建设中，一般认为园区内部是安全的，威胁主要来自外界。在园区边界上，一般使用防火墙、IDS/IPS 作为安全设备。随着安全挑战的不断升级，仅通过传统的安全措施和独立工作的形式进行边界防御已经远远不够了，安全模型需要由被动模式向主动模式转变，从根源－终端彻底解决网络安全问题，提高整个企业的信息安全水平。

目前园区网络安全一般从网络监管、边界防御、接入安全及远程接入等方面进行考虑。接入安全主要指导园区内的安全接入，包括终端安全接入控制，例如：用户隔离，端口隔离等；远程接入涉及分支机构、出差人员对园区内部的安全访问；边界防御通过防火墙、IPS/IDS 对园区出口，园区内的各个组织单元之间进行有效防护和隔离。

网络安全技术

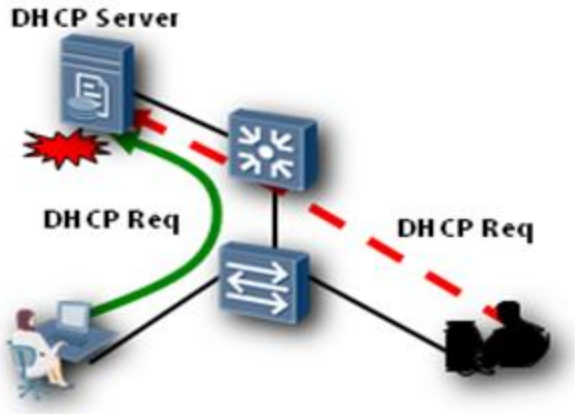
网络的安全是园区网安全最基本的保证。这里主要从交换机的安全特性上的使用来保证网络的安全。包括 DHCP Snooping、ARP 防攻击、MAC 防攻击、IP 源防攻击等。这些安全特性工作于 OSI 模型的链路层，可在接入层交换机上部署。

DHCP Snooping

DHCP Snooping 是 DHCP（Dynamic Host Configuration Protocol）的一种安全特性，通过截获 DHCP Client 和 DHCP Server 之间的 DHCP 报文进行分析处理，可以过滤不信任的 DHCP 报文并建立和维护一个 DHCP Snooping 绑定表。该绑定表包括 MAC 地址、IP 地址、租约时间、绑定类型、VLANID、接口等信息。

DHCP Snooping 部署在二层设备上面，一般部署在接入交换机上。如图 3-19 所示，汇聚交换机上配置 DHCP Relay，在接入交换机上配置 DHCP Snooping，其中上行接口配置为 Trust。

图3-19 DHCP 服务器仿冒示意图



DAI-ARP 欺骗

动态 ARP 检测（Dynamic ARP Inspection）应用在设备的二层接口上，利用 DHCP Snooping 绑定表来防御 ARP 攻击。当设备收到 ARP 报文时，将此 ARP 报文中的源 IP、源 MAC、端口、VLAN 信息和 DHCP Snooping 绑定表的信息进行比较。如果信息匹配，说明是合法用户，则允许此用户的 ARP 报文通过；否则，认为是攻击，丢弃该 ARP 报文。

图3-20 DAI-ARP 欺骗攻击示意图

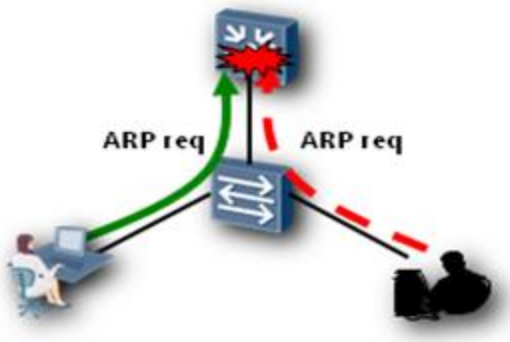
如图 3-20 所示，交换机作为二层设备，用户通过 DHCP 上线。用户上线后，设备会生成相应的 DHCP 绑定表，绑定表包括用户的源 IP、源 MAC、端口、VLAN 信息。当用户发送 ARP 报文时，设备查找此 ARP 信息是否和该用户的绑定表匹配，如果是相同的，则允许报文通过，否则丢弃该 ARP 报文。合法用户存在绑定表，其发送的 ARP 报文会被允许通过，而攻击者发送虚假的 ARP 报文，无法匹配到绑定表，报文被丢弃。

ARP 限速

ARP 报文限速功能是指对上送 CPU 的 ARP 报文进行限速，可以防止大量 ARP 报文对 CPU 进行冲击。例如，在配置了 ARP Detection 功能后，设备会将收到的 ARP 报文重定向到 CPU 进行检查，这样引入了新的问题。如果攻击者恶意构造大量 ARP 报文发往设备，会导致设备的 CPU 负担过重，从而造成其他功能无法正常运行甚至设备瘫痪，这个时候可以启用 ARP 报文限速功能来控制上送 CPU 的 ARP 报文的速率。

图 3-21 给出了 ARP 限速的示意图。当用户发出 ARP 请求的速度在规定范围内的时候，ARP 请求报文可以正常上送，当攻击者以超过允许范围的速度发出 ARP 请求的时候，超过速度范围的报文将被丢弃。

图3-21 ARP 限速示意图



MAC 泛洪

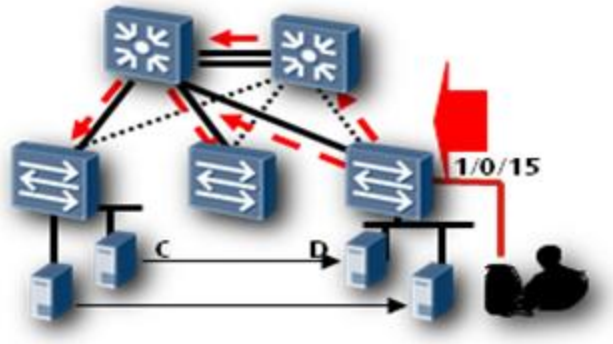
MAC 泛洪攻击是指攻击主机通过程序伪造大量包含随机源 MAC 地址的数据帧发往交换机。有些攻击程序一分钟可以发出十几万条伪造源 MAC 地址的数据帧，交换机根据数据帧中的 MAC 地址进行学习，但一般交换机的 MAC 地址表容量也就几千条，交换机的 MAC 地址表瞬间被伪造的 MAC 地址填满，交换机的 MAC 表填满后，交换机再收到数据，不管是单播、广播还是组播，交换机都不再学习 MAC 地址，如果交换机在 MAC 地址表中找不到目的 MAC 地址对应的端口，交换机就像集线器一样，向所有端口广播数据，这样就可能造成广播风暴。

在华为交换机上，可以通过对 MAC 学习限制及流量抑制的功能来防止 MAC 泛洪攻击。

MAC 学习限制是指限制 MAC 学习的数目。华为交换机支持在接口、VLAN、槽位和 VSI 四个方面对 MAC 学习数目进行限制。同时，华为交换机支持对未知单播、广播及组播流量进行速度限制。通过对 MAC 学习限制及流量抑制，可以有效地防范 MAC 泛洪攻击。

图 3-22 给出了 MAC 泛洪攻击的示意图，图中，假设攻击者发出一个伪造目的 MAC 的报文，交换机收到报文后发现找不到目的 MAC 就会向除接收端口的所有端口发送此报文，导致此报文在广播域内广播。如果攻击者发送大量的报文，就可能会造成网络中断或瘫痪。

图3-22 MAC 泛洪攻击示意图

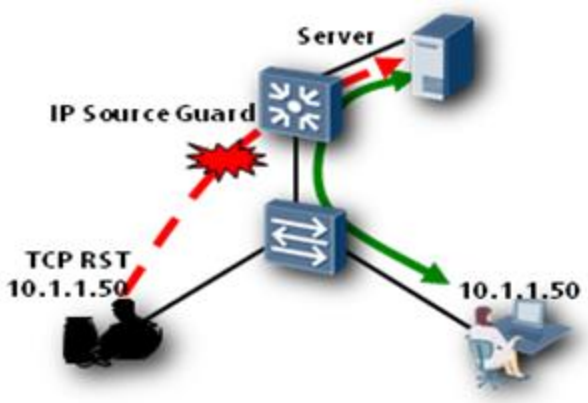


IP Source Guard

IP 源地址防护能够限制二层不信任端口的 IP 流量。它采取的方法是，通过 DHCP 绑定表或手动绑定的 IP 源地址来对 IP 流量实行过滤此特性可以阻止 IP 地址欺骗攻击，也就是主机通过把自己的源 IP 地址修改成其他主机的 IP 地址实现的攻击。任何从不信任的端口入站的 IP 流量，只要其源地址与指定(DHCP Snooping 或静态绑定表)的 IP 地址不同，就会被过滤掉。

IP 源地址与防护特性需要在不信任的二层接口上和 DHCP Snooping 共同使用。IP 源地址防护会生成一个 IP 源地址绑定表，并且对这个列表进行维护。这个列表既可以通过 DHCP 学习到也可以手动配置。列表中的每个条目都包括 IP 地址及与这个 IP 地址所关联的 MAC 地址及 VLANID。

图3-23 IP Source Guard 功能示意图



如图 3-23 所示，在接入交换机上使能 IP Source Guard 功能。此时，合法用户的 IP 地址、MAC 地址及 VLAN 信息能满足绑定表的信息，用户能正常访问网络。而非法用户发出的报文却会在接口上被丢弃，进而阻止了非法用户危害网络安全。

MFF 技术

园区网络中，通常使用 MFF（MAC-Forced Forwarding）实现不同客户端主机之间的二层隔离和三层互通。MFF 截获用户的 ARP 请求报文，通过 ARP 代答机制，回复网关 MAC 地址的 ARP 应答报文。通过这种方式，可以强制用户将所有流量（包括同一子网内的流量）发送到网关，使网关可以监控数据流量，防止用户之间的恶意攻击，能更好的保障网络部署的安全性。

MFF 特性包括两种接口角色：

- 用户接口

  MFF 的用户接口是指直接接入网络终端用户的接口。

  用户接口上对于不同的报文处理如下：

  - 允许协议报文通过。
  - 对于 ARP 和 DHCP 报文上送 CPU 进行处理。
  - 若已经学习到网关 MAC 地址，则仅允许目的 MAC 地址为网关 MAC 地址的单播报文通过，其他报文都将被丢弃；若没有学习到网关 MAC 地址，目的 MAC 地址为网关 MAC 地址的单播报文也被丢弃。
  - 组播数据和广播报文都不允许通过。
- 网络接口

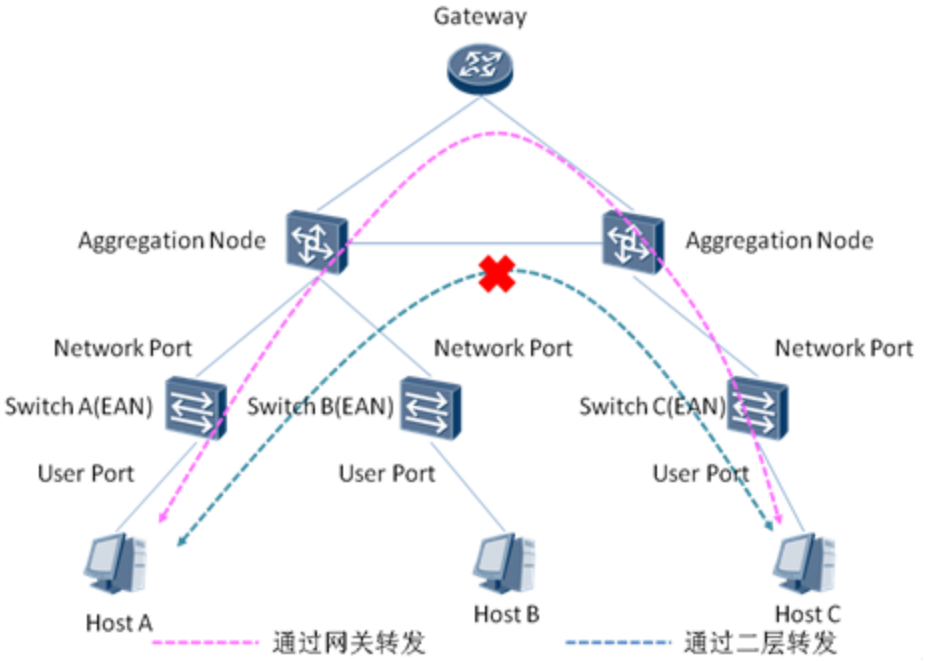
  MFF 的网络接口是指连接其他网络设备（如：接入交换机、汇聚交换机或网关）的接口。

  网络接口上对于不同的报文处理如下：

  - 允许组播报文和 DHCP 报文通过。
  - 对于 ARP 报文则上送 CPU 进行处理。
  - 其他广播报文都不允许通过。

图 3-24 给出了 MFF 方案的典型应用场景。当交换机 A、B 和 C 上启用了 MFF 功能后，主机 A 与主机 C 之间可以通过三层进行转发，不能通过二层转发。所有主机 A 与 C 之间的流量，都会先经过网关，然后再进行转发。

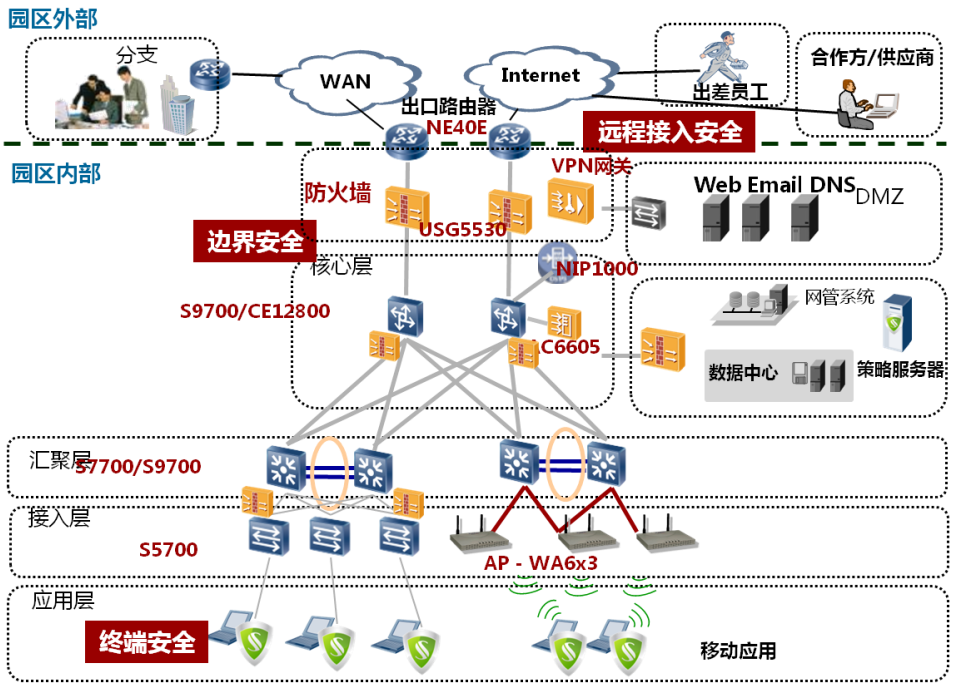
图3-24 MFF 方案的应用场景



3.8.2 华为安全解决方案全景图

如图 3-25，华为金融园区安全解决方案分为如下三部分：

图3-25 华为金融园区安全解决方案全景图



边界安全：园区出口，不同物理分区及不同业务分区之间的隔离和访问控制

用户终端安全：终端用户的认证、访问策略控制、权限管理等

远程接入安全：分支和移动用户，通过 internet 访问内网，确保数据交互安全

3.8.3 边界安全规划

边界防护概述

所谓网络边界，是指园区网络与其他网络的分界线。

对边界进行安全防护，首先必须明确哪些网络边界需要防护，这可以通过安全分区设计来确定。定义安全分区的原则就是首先需要根据业务和信息敏感度定义安全资产，其次对安全资产定义安全策略和安全级别，对于安全策略和级别相同的安全资产，就可以认为属于同一安全区域。

网络边界是网络的重要组成部分，负责对网络流量进行最初及最后的过滤，因此边界安全的有效部署对整网安全意义重大。

边界防护安全设计

一般而言，一个完整的安全部署包括边界路由器、边界防火墙、IPS、边界防毒墙、边界流量分析监控等安全部件及各安全部件之间的协同工作。这些部件仅仅依靠各自自身的力量是无法提供完整的网络安全。只有这些部件的功能相互补充，相互结合，协同工作才能形成一个立体的防御结构。

- 边界路由器

  路由器在网络中承担路由转发的功能，它们将流量引导进入网络、流出网络或者在网络中传输，由于边界路由器具有丰富的网络接口，一般置于 Internet 出口或广域网出口，是流量进入和流出之前我们可以控制的第一道防线。

- 边界防火墙

  防火墙设备通过一组规则决定哪些流量可以通过而哪些流量不能通过防火墙。防火墙可以对边界路由器不能监控的流量进行更加深入地分析和过滤，并能够按照管理者所确定的策略来阻塞或者允许流量经过。

  华为 Eudemon 系列防火墙支持安全域管理、攻击防范、ASPF、NAT 等功能，通过这些功能保障网络安全。

  - 安全域管理

    华为防火墙采用基于安全区域的隔离模型，每个安全区域可以按照网络的实际组网加入任意接口，因此防火墙的安全管理模型不会受到网络拓扑的影响。

    不同的安全区域之间的访问设计不同的安全策略组（ACL 访问控制列表），每条安全策略组支持若干个独立的规则。这样的规则体系使得统一安全网关的策略十分容易管理，方便用户对各种逻辑安全区域的独立管理。

    基于安全区域的策略控制模型，可以清晰地分别定义从 trust 到 untrust、从 DMZ 到 untrust 之间的各种访问，这样的策略控制模型使得华为统一安全网关的网络隔离功能具有很好的管理能力。

  - 攻击防范

    攻击防范功能是防火墙必备的功能之一，常见的攻击类型有 DOS 攻击、扫描窥探攻击、畸形报文攻击等等。

- ASPF 过滤技术

  ASPF 是一种高级通信过滤技术，它检查应用层协议信息并且监控基于连接的应用层协议状态。防火墙依靠这种基于报文内容的访问控制，能够对应用层的一部分攻击加以检测和防范，包括对于 FTP、HTTP、RTSP、SIP 等的检测。

- NAT

  NAT 的基本原理是仅在私网主机需要访问 Internet 时才会分配到合法的公网地址，而在内部互联时则使用私网地址。

  当访问 Internet 的报文经过 NAT 网关时，NAT 网关会用一个合法的公网地址替换原报文中的源 IP 地址，并对这种转换进行记录；之后，当报文从 Internet 侧返回时，NAT 网关查找原有的记录，将报文的目的地址再替换回原来的私网地址，并送回发出请求的主机。这样，在私网侧或公网侧设备看来，这个过程与普通的网络访问并没有任何的区别。在实现方式上，NAT 可以分为 Basic NAT、NAPT 方式、NAT Server 方式、EASY IP 方式、DNS Mapping 方式等。

- P2P 流量检测和流量控制

  防火墙支持的 P2P 流量检测和流量控制功能：

- 支持基于规则文件的特征检测和行为检测，规则文件可以升级更新
- 支持基于 ACL 的用户策略控制
- 支持上下行的不同限流
- 支持协议优先级的动态调整
- 支持各种协议检测的打开和关闭
- 支持基于时间段的分时段限流

  对 P2P 流量可以限定在一个范围内，这样不但可以使得用户自由的使用 P2P 软件，也不会造成因为 P2P 流量对网络造成太大的冲击。

  例如：支持迅雷、沸点、BT、Kugoo、PPGou、Poco/pp、Baibao、BitComet、Kazaa/FastTrack、Emule/eDonkey、PPSTREAM、UUSee、PPLive、QQLive、TVAnts、BBSEE、Vagaa、Mysee、Filetopia、Soulseek 等 P2P 协议检测和流量控制。

- URL 过滤

  华为防火墙的 URL 过滤功能采用了先进的模式匹配引擎算法，大大减少了 URL 匹配的时间，凭借先进的软硬件性能，能够快速地处理大量的 URL 访问请求。

  防火墙支持远程 URL 分类服务器，远程 URL 分类服务器提供了细粒度的 URL 资源种类，使用全面而准确的后台 URL 资源分类数据库，自动化地实现对用户访问 URL 的自动分类。另外，防火墙支持本地 URL 分类功能，用户可以自定义个性化 URL 资源访问控制的功能。并且可以将 URL 访问控制策略和时间、IP 地址、分类访问控制列表等关键策略进行关联，从而实现基于时间、用户和访问类别等策略的 URL 过滤功能。

  另外，防火墙支持本地 URL 黑/白名单功能，支持基于前缀匹配、后缀匹配、关键字匹配、精确匹配和参数匹配等。

- IPS/IDS

  随着互联网的不断发展，黑客攻击技术也出现了许多新的变化，这也促使网络安全产品不断的更新换代。一种新型的安全防护产品-网络入侵防御系统应运而生。网络入侵防御系统作为一种在线部署的产品，其设计目标旨在准确监测网络异常流量，自动对各类攻击性的流量，尤其是应用层的威胁进行实时阻断，而不是在监测到恶意流量的同时或之后才发出告警。这类产品弥补了防火墙、

入侵检测等产品的不足，提供动态的、深度的、主动的安全防御，为企业提供了一个全新的入侵保护解决方案。

IPS 安全网关产品可以部署在企业网络出口处或者重要服务器前面，提供主动的、实时的防护。准确检测 2 到 7 层的网络异常流量，自动对各类攻击的流量，尤其是应用层的威胁进行实时阻断。

IPS 系统自身的安全非常重要，必须能够抵御那些常规的网络安全威胁：如病毒的感染、蠕虫的传播，不可使用通用的处理器及操作系统等。这些都有周知的漏洞，很容易被利用进行入侵攻击。而 IPS 的检测粒度非常细，由此系统必须具备高性能的数据报处理及转发能力，不然低效的 IPS 系统将成为网络的性能瓶颈。

网络上很多应用服务器（如 HTTP、SMTP、FTP、POP3、IMAP4、MSRPC、NETBIOS、SMB、MS_SQL、TELNET、IRC、DNS 等）在设计中并不完善，如对协议中的异常情况考虑不足。因此黑客常利用协议的漏洞对服务器发起攻击。他们向服务器发送非标准或者缓冲区溢出的协议数据，从而夺取服务器控制权或者造成服务器宕机。IPS 能够检测、识别网络流量的协议异常（包括协议遵从性、参数合法性等）并加以阻断。

网络中常包含大量黑客攻击、病毒、特洛伊木马、恶意软件等恶意流量。这些恶意流量都有各自不同的签名（特征）。因此，必须有专业的安全分析工程师对这些恶意网络流量进行深入分析，提取相应的特征码并形成签名。IPS 根据签名库，使用特征检测引擎对网络中传输的数据包进行高速匹配，从而对命中签名规则的流量进行阻断等方式进行响应动作。

IPS 的检测引擎和签名库，对于入侵检测的效果具有重要意义。优秀的检测引擎算法极大程度影响检测的速度；全面而准确的签名库能够有效防御大量威胁，减少误报。有了优秀的检测引擎及签名库，IPS 能够更好的检测各类攻击，如最新病毒、特洛伊木马、恶意软件等进行检测防御。

IPS 的特征检测引擎和签名库必须支持有效升级，以保证能够应对不断变化着的网络威胁。

通常情况下，IPS 设备的工作步骤如下：

- 捕获网络数据包
- 重组数据包，包括流重组和分片重组
- 对数据包进行协议识别，有基于端口的识别和基于内容的识别
- 将数据包送入检测引擎匹配
- 最后根据引擎检测结果及安全策略采取响应动作

所谓 IDS 联动，指 IDS 设备能自动侦听整个网络中是否存在恶意攻击、入侵或其他安全隐患行为，通过下发指令的方式通知防火墙，由防火墙对攻击报文进行丢弃或其它处理。采用 IDS 联动方式进行攻击防范，入侵检测和攻击处理两个过程有效分离，充分发挥了各设备的优势，改善了系统性能。

华为防火墙除了自身提供强劲的攻击防范能力外，还能够和专业的 IDS（Intrusion Detective System）设备联合组网，即 IDS 设备外置。由于 IDS 设备包含非常完备的攻击行为信息，因此联合组网将充分发挥 IDS 设备高效、全面的安全保障能力。

通过和 IDS 设备联动，防火墙可以提供一种高可靠的主动防御模型。通过这种主动防御的模型，提供了高可靠的安全解决方案。

用户先配置好基本的静态安全策略，通过 IDS 设备可以动态发现安全隐患，通过防火墙设备修改安全策略，起到实时、动态的修改防御策略，保证了整网的安全。

华为防火墙提供灵活的联动接口协议，可以和很多 IDS 设备互通，方便地支持各种 IDS 设备和防火墙联合工作。

- 边界防病毒

  近年来计算机病毒趁着网络信息化的热潮，不断骚扰和破坏人们正常的工作秩序。病毒已逐渐成为网络安全的祸首，严重的病毒爆发将直接导致网络的瘫痪，在边界安全防护中也同样要考虑对病毒的防护。

  华为防火墙提供了 Anti-Virus 防病毒功能，防病毒功能采用了先进的病毒检测引擎和病毒库，病毒检出率非常之高。

  防火墙的病毒引擎支持启发式扫描，对网络上传输的代码文件进行深入的行为分析，采取对需要扫描的文件进行逻辑分析以及行为分析，通过这种方式，可以很大程度的发现一些行为异常的程序，发现未知的病毒。

  遍布全球的病毒检测点和和专业病毒分析团队，可以实时发现网络最新病毒，并且通过病毒分析团队确认和分析病毒特征，及时的生成最新病毒库。防火墙通过可以多种方式升级或更新病毒库，实现病毒的实时检测。病毒库支持自动定时升级、实时升级、本地升级和回退功能。

边界防护组网设计

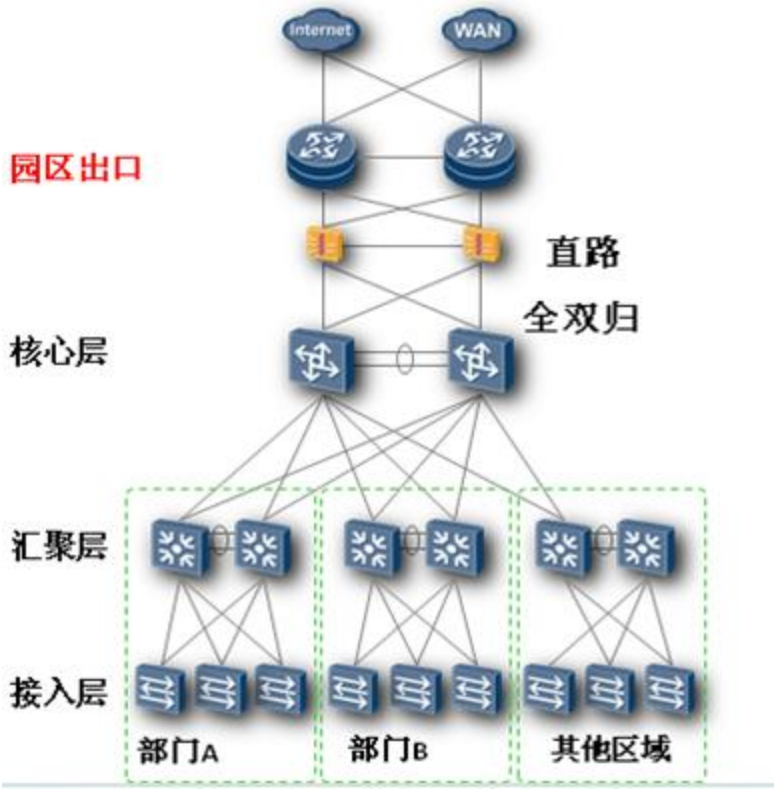
由于防火墙与 IPS/IDS 等一般是部署在同一个地方，且华为防火墙同时支持防火墙与 IPS 功能，因此，边界组网设计图中仅画出防火墙。

- Internet 网络出口防护

  对金融企业总部或大型分支机构，一般在园区出口部署双防火墙，两防火墙呈主备或负载均衡的方式工作。如图 3-26 所示，在核心交换机与园区路由器之间采用直路全双归方式接入防火墙设备，两台防火墙设备之间采用主备或负载均衡方式连接。这样，园区出口路由器、防火墙及核心路由器之间都有备份作用，保证了链路的可靠性。防火墙 E8000E 放置在总部出口，主要承担以下功能:

  - 启用防火墙攻击防范以及访问控制，抵御外来的各种攻击。
  - 根据需要启用地址转换功能，满足出口公网不足的需要。
  - 根据需要开启虚拟防火墙功能，通过不同的虚拟防火墙与各大客户对应，将不同的服务器群用 VPN 隔离开。
  - 启用 L2TP VPN 的功能，允许出差移动用户通过拨号的方式接入不同的 VPN，访问不同 VPN 里的业务或者设备。

图3-26 园区出口典型组网



除了直路全双归，防火墙的接入方式还有与交换机双归，与路由器口字型、与交换机路由器都口字型及旁挂。

图3-27 防火墙出口连接方式-与交换机双归、与路由器口子型

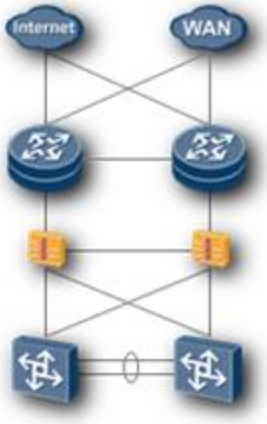


图3-28 防火墙出口连接方式-与交换机口子型、与路由器口子型

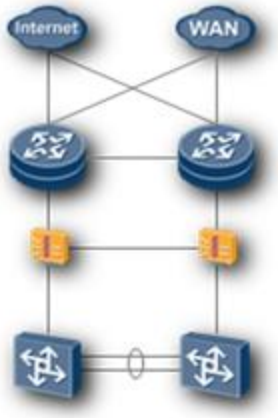


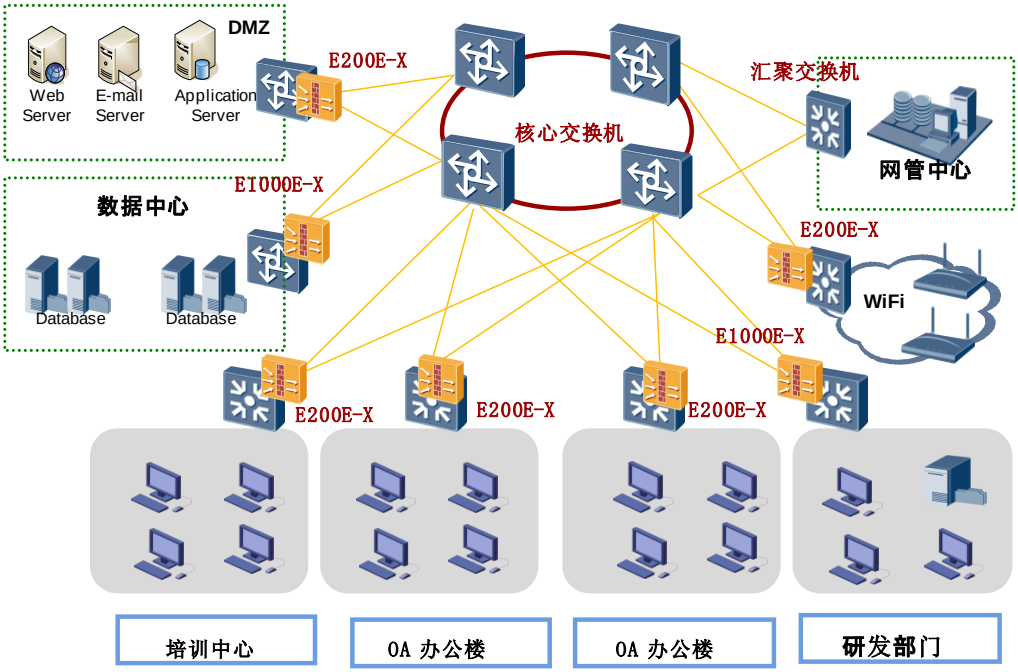
图3-29 防火墙出口连接方式-旁挂

- 域间防护

  园区出口部署的防火墙可以解决园区内部网络与外部网络之间的安全问题，但研究表明，80%的网络安全漏洞都存在于内部网络。因此，内部的安全防护更为重要。当网络划分安全区域后，在不同信任级别的安全区域之间就形成了网络边界。

  在园区网内部，不同的业务部门、研发中心、办公中心可能都具有不同的安全策略。从安全的角度讲，在各个不同的部门、研发中心、办公中心、数据中心、DMZ 区域的出口都部署防火墙是最理想的。也可以在核心层部署防火墙，将各业务部门划分在不同的 VPN 中，防火墙采用虚拟防火墙的方式管理各安全域的安全策略。

图3-30 园区网内部边界防护示意图



3.8.4 远程接入安全规划

随着企业的发展及企业的信息化建设，分支机构、出差员工远程接入已经成为一个不可避免的情况。针对企业园区的大型、小型分支机构、出差员工及合作方伙伴的接入提供远程接入方式。

在园区网组网规划中，可以采用专线与 Internet 两种方式接入。

专线接入

对于专线接入，运营商一般会有 ADSL（Asymmetric Digital Subscriber Line）接入、SDH（Synchronous Digital Hierarchy）接入、PON（PassiveOpticalNetwork）接入等。

- Modem/ISDN

  典型的电路交换网络系统。后者能够以普通的铜缆电话线路实现比前者更高速率和质量的数据及语言的传输。当然这两者还都是比较低速的接入方式，前者理论极限带宽为 56kbps，后者提供了 128kbps 的基本速率接口以及较高速率的 T1（1.544Mbit/s）、E1（2.048Mbit/s）接口。当然无论是 modem 还是 ISDN 接入，在现在看来都是不可接受的，根本无法承担起当前的业务需求。

- xDSL 接入

  xDSL 接入是以铜质电话线为传输介质的传输技术组合。它包括 HDSL、SDSL、VDSL、ADSL 等，一般统称为 xDSL。它们主要的区别就是体现在信号传输速度和距离的不同以及上行速率和下行速率对称性的不同这两个方面。

  ADSL 是国内的主流接入技术，因具有下行速率高、频带宽、性能优等特点而深受广大用户的喜爱，成为继 Modem、ISDN 之后的一种全新的更快捷、更高效的接入

方式。并且得益于其承载的电话线路的广阔性和成熟性，用户接入基本上不需要更改网络，从而在管理维护上具有相当的优势。

HDSL 与 SDSL 支持对称的 T1/E1（1.544Mbps/2.048Mbps）传输。其中 HDSL 的有效传输距离为 3 到 4 公里，且需要两至四对铜质双绞电话线；SDSL 最大有效传输距离为 3 公里，只需一对铜线。比较而言，对称 DSL 更适用于企业点对点连接应用，如文件传输、视频会议等收发数据量大致相应的工作。同非对称 DSL 相比，对称 DSL 的市场要少得多。

VDSL、ADSL 属于非对称式传输。其中 VDSL 技术是 xDSL 技术中最快的一种，在一对铜质双绞电话线上，下行数据的速率为 13 到 52Mbps，上行数据的速率为 1.5 到 2.3Mbps，但是 VDSL 的传输距离只在几百米以内，VDSL 可以成为光纤到家的具有高性价比的替代方案。从当前 xDSL 的这些特点可以看出，其主要应用于网上高速冲浪、视频点播（IAV）、远程局域网络（LAN）访问等业务，因为在这些应用中用户下载的信息往往比上载的信息（发送指令）要多得多。

- SDH 接入

  SDH 是一种将复接、线路传输及交换功能融为一体，并由统一网管系统操作的综合信息传送网络，是美国贝尔通信技术研究所提出来的同步光网络（SONET）。国际电话电报咨询委员会（CCITT）（现 ITU-T）于 1988 年接受了 SONET 概念并重新命名为 SDH，使其成为不仅适用于光纤也适用于微波和卫星传输的通用技术体制。它可实现网络有效管理、实时业务监控、动态网络维护、不同厂商设备间的互通等多项功能，能大大提高网络资源利用率、降低管理及维护费用、实现灵活可靠和高效的网络运行与维护，因此是当今世界信息领域在传输技术方面的发展和应用的热点，受到人们的广泛重视。

- PON 接入

  PON 接入主要是为了应对当前层出不穷的各种新业务，满足人们对网络接入带宽日益增长的需求。据相关数据分析，未来 3 年，用户的平均带宽需求将超过 10M。与其他有线、无线接入技术相比，光纤接入在带宽容量、扩展潜力和覆盖距离方面具有很大的优势。随着光纤光缆的发展和技术的成熟，PON 接入的成本也快速下降，由此，接入网络的光纤化也逐渐成为现实。

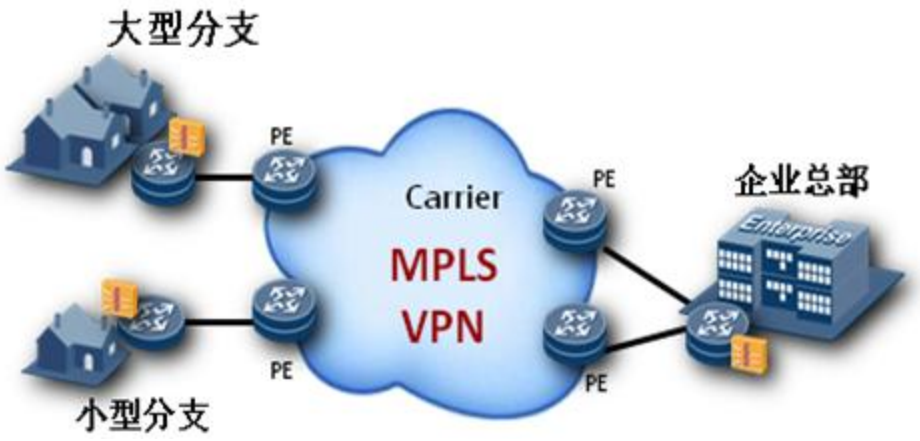
  不同于点对点的光纤接入，PON 采用了点对多点的方式，减少了端局的激光器（端口）数量以及相应的光纤线路，大大降低了使用成本。

- VPN 接入

  对于没有广域专网的企业，通过运营商提供的 MPLS VPN 实现互联租用运营商固定专线的企业，可以通过 MPLS VPN 实现内部业务隔离和互访。垂直行业通过自己的专网部署 MPLS VPN 互通，PE 部署在企业出口路由器。

  多园区互联的典型场景如图 3-31 所示。

图3-31 多园区互联场景示意图-MPLS VPN

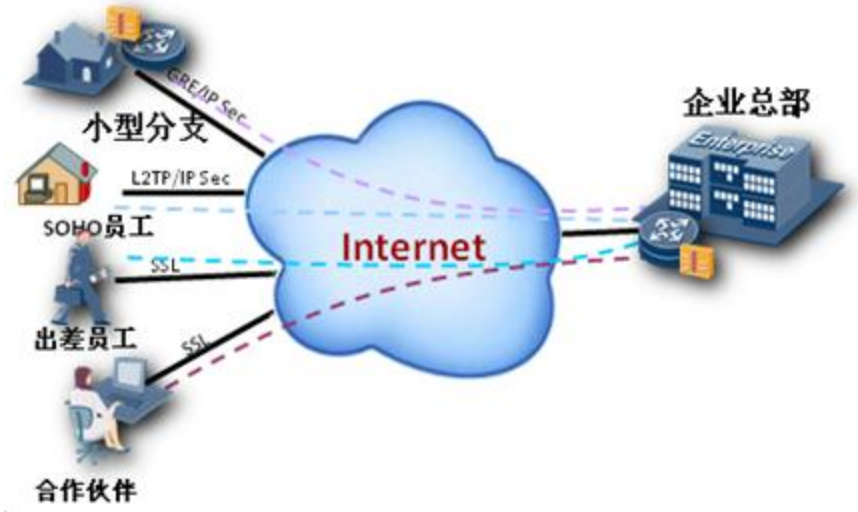


在 MPLS VPN 网络中，MPLS 域内部的节点（P 及 PE 设备）是通过普通的 IGP 路由协议实现连通的，而各 PE 设备之间是通过 BGP 扩展，即 MP-BGP 实现的，所以，在路由规划上，每个 MPLS 域会单独划为一个 AS 域，内部运行普通的 IGP 协议保证整个 MPLS 域的连通，PE 设备需运行 BGP 路由协议用于扩散 VPN 私网路由信息。PE 和 CE 之间可以通过静态路由，动态路由 IGP（如 RIP，OSPF 等，需要多实例化）或 EBGP 交换 VPN 路由。

Internet 远程接入

除采用 MPLS VPN 对分支机构与总部进行连接外，小型分支机构，SOHO 员工，出差员工及合作伙伴也可以以 GRE over IPsec、L2TP over IPsec、SSL 方式通过 Internet 接入企业网总部。通过 Internet 接入园区网内部的示意图如图 3-32 所示。

图3-32 Internet 远程接入场景



- GRE over IPsec

IPsecVPN 是互联网工程任务组（IETF）定义的标准，可以保障信息的机密性、完整性，并实现身份认证。IPsec 通过 OSI 参考模型的第 3 层（网络层）来保护网络，从而保护 IP 网络上所有的应用和通信。

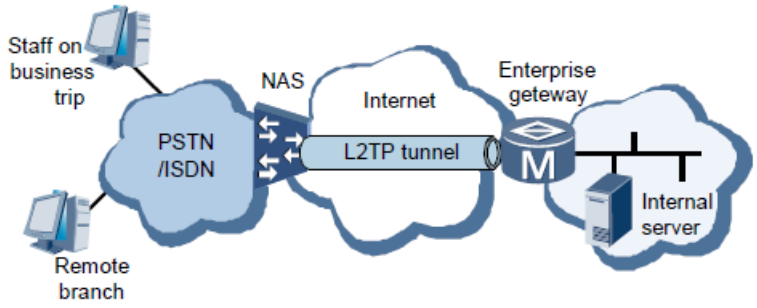
通过 GRE over IPSec，可以弥补 IPSec 协议的不足，在 GRE Tunnel 上部署路由协议，在 Tunnel 端点，针对 IPSec 服务，仅配置对 GRE 流量的保护。GRE over IPSec 可大大提升组网的灵活性。

GRE 能够封装路由协议,但是单纯的 password 不能解决在公网上面安全性的问题。而 IPSec 只支持 IP 协议，由于 IPSec 隧道不能承载路由协议，所以对 VPN 的扩展性造成了很大的影响。所以如果把 GRE 和 IPSec 完美的结合起来，不仅可以解决 VPN 扩展性的问题,同时也能解决安全性的目的。

- L2TP over IPsec

  L2TP 是 PPP 拨号业务的延伸。PPP 拨号要求用户侧和接入服务器之间二层可达，对于企业跨广域的连接是不现实的。L2TP 通过引入 LAC 和 LNS 解决了这一问题。

图3-33 分支 L2TP 接入示意图



传统的 L2TP VPN 中 NAS 设备是运营商的，这样企业所有的分支都要在运营商的 NAS 上配置业务。如果分支点很多，业务开通费用会比较高。为了解决这个问题，出现了另一种方式。这种方式是在企业分支内部部署设备作为 NAS，分支内部用户采用 PPP 拨号，与运营商无关。采用这种方式和在分支内采用 DHCP 方式主要区别在于用 L2TP 具有基于用户的认证功能，安全性相对较高。如果分支网络没有其它的用户认证手段，可以利用 L2TP 的这一优点；如果分支网络有其它用户认证手段，则不推荐使用 L2TP（因为其报文封装效率低，相同情况下会占用更多 WAN 带宽）。

与 GRE 类似，由于 L2TP 本身没有加密功能，因此如果使用 L2TP，要保证分支网络的数据安全，则要和 IPSec 结合使用，即 L2TP over IPSec。

- SSL VPN

  SSL VPN 是以 HTTPS（Secure HTTP，安全的 HTTP，即支持 SSL 的 HTTP 协议）为基础的 VPN 技术，工作在传输层和应用层之间。SSL VPN 充分利用了 SSL 协议提供的基于证书的身份认证、数据加密和消息完整性验证机制，可以为应用层之间的通信建立安全连接。

  SSL VPN 广泛应用于基于 Web 的远程安全接入，为用户远程访问公司内部网络提供了安全保证。

  管理员在 SSL VPN 网关上创建企业网内服务器对应的资源。远程接入用户访问企业网内的服务器时，首先与 SSL VPN 网关建立 HTTPS 连接，选择需要访问的资源，由 SSL VPN 网关将资源访问请求转发给企业网内的服务器。SSL VPN 通过在远程

接入用户和 SSL VPN 网关之间建立 SSL 连接，SSL VPN 网关对用户进行身份认证等机制，实现了对企业网内服务器的保护。

SSL VPN 可以按照无客户端模式、瘦客户端模式和胖客户端模式进行部署。

- 使用无客户端模式，可以安全地访问 Web 资源和基于 Web 的内容。这种模式对于可通过 Web 浏览器访问的内容非常有用。
- 瘦客户端模式提供基于 TCP 服务的远程访问，如 POP3、SMTP、IMAP、Telnet 和 SSH。瘦客户端通过 Java 小程序进行传输，Java 小程序在会话建立后通过 SSL VPN 动态下载。该模式扩展了 Web 浏览器的加密功能。
- 胖客户端模式可提供去往大量应用的远程访问，从 VPN 服务器下载 SSL VPN 客户端，就可以实现动态传输。该模式提供了一个轻量组、集中配置并且兼容性良好的 SSL VPN 隧道客户端，从而实现对几乎所有应用的全网络访问。

3.8.5 终端安全规划

终端安全概述

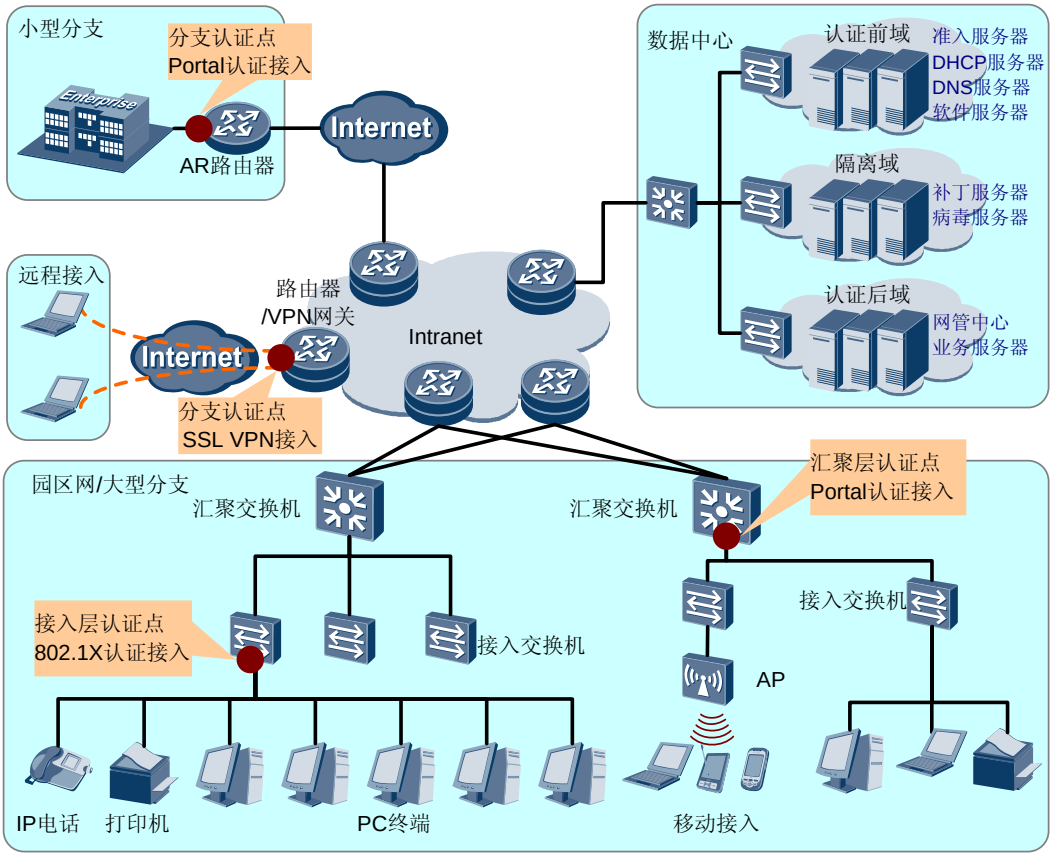
华为的 NAC（Network Access Control）安全解决方案以“只有合法的用户、安全的终端才可以接入网络”为主导思想。以全系列的企业网络和安全产品，结合 TSM（Terminal Security Management）系统，提供以“用户认证、安全检查、修复升级”为基础的全面安全的 NAC 解决方案，并提供了丰富扩展特性，为企业网络提供了整体终端安全防护能力。

华为 NAC 方案具有以下特点：

- 身份认证和访问控制
- 接入安全检查和控制
- 系统修复与升级
- 行为管理
- 软件分发
- 资产管理

华为的终端安全解决方案如图 3-34 所示，从接入网络的终端安全控制入手，将终端安全状况和网络准入控制结合在一起，通过检查、隔离、加固和审计等手段，加强网络用户终端的主动防御能力，保证企业中每个终端的安全性，保护企业网络的安全性。

图3-34 终端安全解决方案示意图



华为终端安全解决方案包括如下内容：

- 通过多种身份认证方式确认终端用户的合法性。
- 绑定检查终端的安全漏洞、终端杀毒软件的安装和病毒库更新。
- 通过统一接入策略和安全策略管理，控制终端用户的网络访问权限。
- 通过桌面运维，完成进行桌面资产注册监控、外设管理和软件分发。

终端认证协议

华为终端准入方案支持 802.1x、MAC 认证、Portal 认证等多种网络访问控制方式，并可灵活部署在用户网络的接入交换机、汇聚交换机、无线控制器、AR 等多种网络设备上，配合 NAC 的终端代理和服务器共同完成 NAC 控制，为园区网提供安全可靠的访问控制。

- 802.1x 认证

  标准的 802.1x 协议是一种基于端口的网络接入控制协议，用于在局域网接入设备的端口一级对所接入的用户设备进行认证和控制。连接在端口上的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源。

  802.1x 认证使用 EAP（Extensible Authentication Protocol）认证协议，实现客户端、设备端和认证服务器之间认证信息的交换。在客户端与设备端之间，EAP 协议报文使用 EAPoL（EAP over LAN）封装格式，直接承载于 LAN 环境中。

- Portal 认证

  Portal 认证是一种三层认证方式。用户可以通过访问 Portal 服务器（Web 服务器）上的 Web 认证页面，输入用户帐号信息，实现对终端用户身份的认证。采用 Portal 认证，用户可以无需安装客户端软件，用户访问 Portal 页面时，通过自动提示下载的 ActiveX 控件实现基本安全检查功能。

  Portal 认证支持 Web 认证且可以无需安装客户端软件，这两个特性使得 Portal 认证对于访客和出差用户具有很好的支持。

- MAC 认证

  对某些特殊情况，终端用户不想或不能通过输入用户帐号信息的方式完成认证。例如某些特权终端希望能“免认证”直接访问网络；对于某些特殊的 PC 终端，如打印机、IP 电话等设备，无法安装客户端软件，也无法通过输入用户帐号信息的方式进行认证授权。此时，可以采用 MAC 认证的方式实现对终端的网络访问控制。

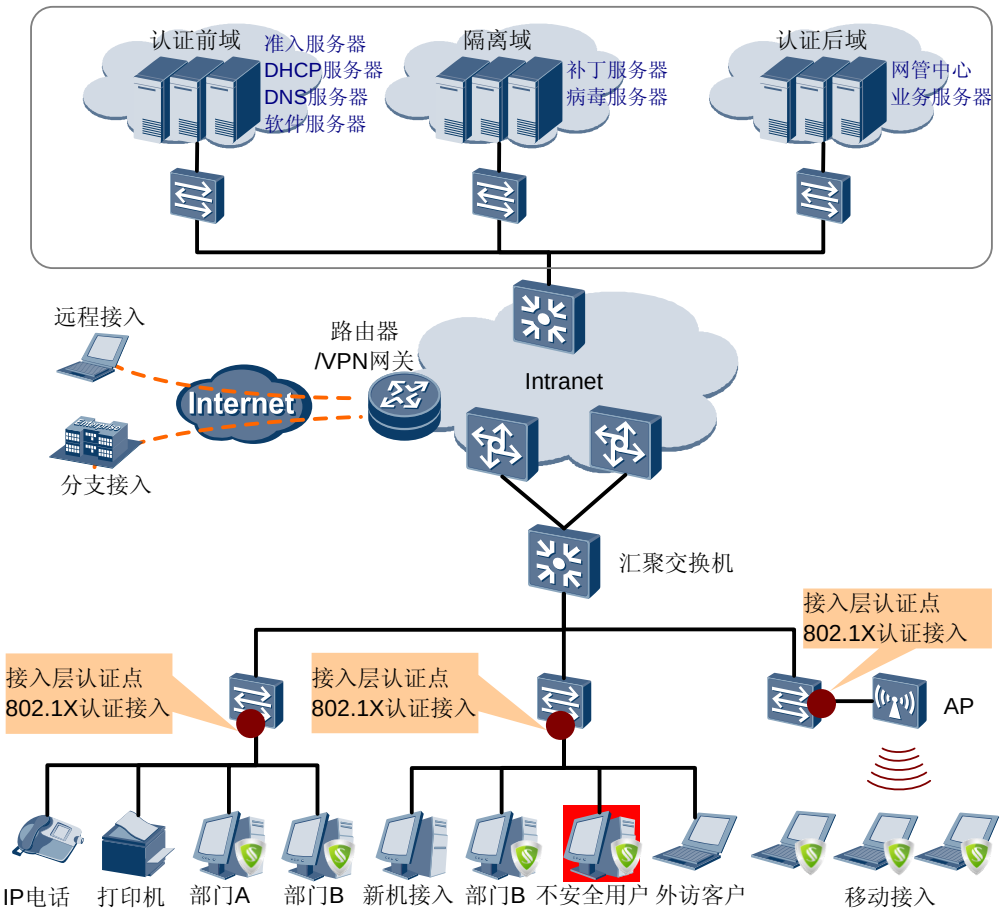
  MAC 认证就是以终端的 MAC 地址作为身份凭据到系统进行认证。启用 MAC 认证后，当终端接入网络时，网络准入设备提取终端 MAC 地址，并将该 MAC 地址作为用户名和密码进行认证。如果认证失败使用户下线，并保持一段时间内不再发起认证和探测，超时后重新开始探测过程；如果认证成功，交换机将增加该 MAC 地址进入 MAC 表，用户将可以正常访问网络。

接入层认证方案规划

目前的安全解决方案专注于保护网络的第三层及以上。然而，危及第二层安全的任何行为都将会危害到整个网络，因此接入层是部署网络安全控制的最佳点。使用 802.1x 身份认证可以直接将非法用户在接入层隔离，确保接入用户的合法性。

接入层认证方案采用传统的三层网络结构，接入层交换机部署 802.1x 认证或 MAC 认证，对接入用户进行身份认证，隔离非法用户和不安全用户。汇聚交换机上配置 ACL 控制访问权限。服务器区除了部署传统的业务服务器、网络管理服务器、DHCP/DNS 服务器外，还需要部署准入服务器以及补丁、病毒服务器。如图 3-35 所示。

图3-35 接入层认证方案组网图



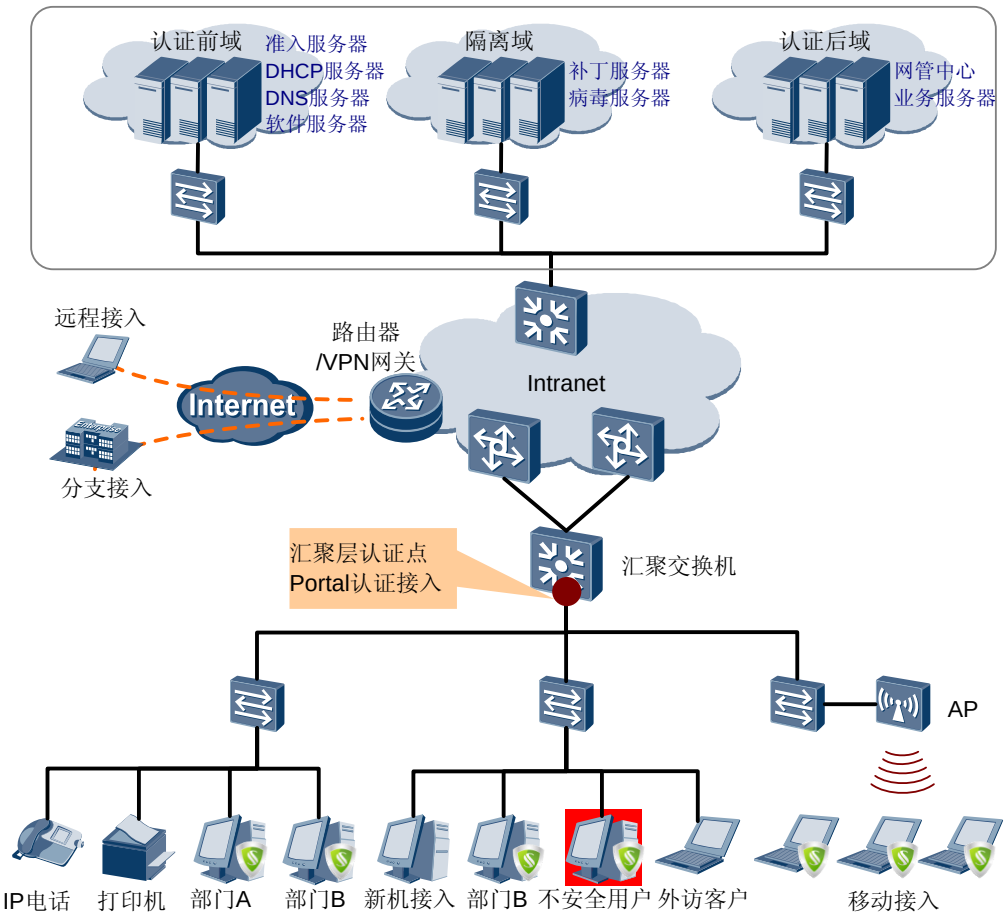
汇聚层认证方案规划

汇聚层部署认证控制点适用于接入用户分散、接入终端类型较多、无线有线混合接入的场景，认证协议建议采用基于网关的 Portal 认证。

这种认证方式与接入层设备无关，终端设备既可以安装代理客户端，也可以不安装（Web 强推方式），适应各种终端接入（PC、手持设备等），方便灵活，管理维护方便。旧网改造中若需要增加安全接入控制功能，而又不希望改变原来网络结构，可以直接在汇聚层部署 Portal 认证。

汇聚层认证方案采用传统的三层网络结构，在汇聚层交换机基于网关部署 Portal 认证，对接入的用户进行身份认证，隔离非法用户和不安全用户。汇聚交换机上配置 ACL 控制访问权限。服务器区除了部署传统的业务服务器、网络管理服务器、DHCP/DNS 服务器外，还需要部署准入服务器以及补丁、病毒服务器。如图 3-36 所示。

图3-36 汇聚层认证方案组网图



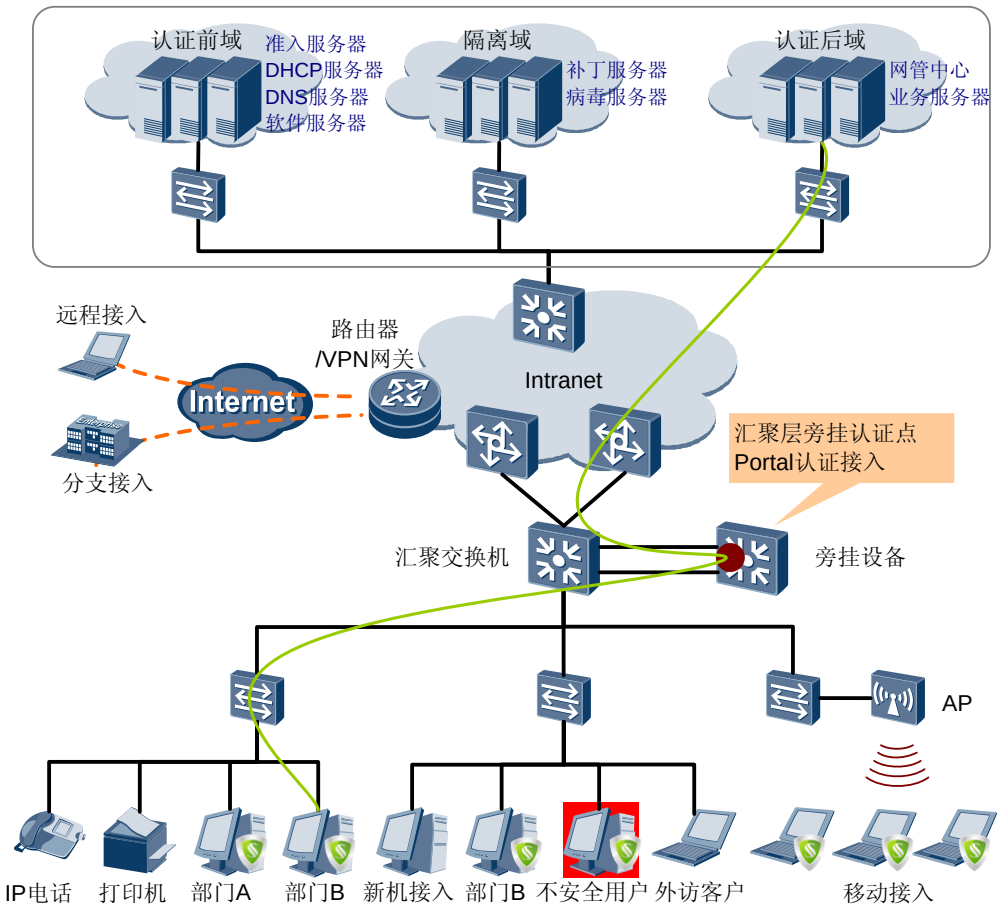
汇聚层旁挂认证方案

汇聚层旁挂认证方案主要针对那些网络设备较为老旧的网络升级场景，不需要改变原有网络结构，旁挂一台设备即可引入一整套的网络安全接入控制方案，能够有效节约用户投资。本方案中，上下行流量都以旁挂设备为网关，对旁挂设备的性能要求较高。

汇聚层旁挂方案仍然推荐使用 Portal 认证方式，具体的 NAC 系统规划、安全策略规划、用户权限规划和可靠性规划都和汇聚层认证按相同。本节不再详述。

如图 3-37 所示，网络结构与汇聚层认证方案类似，不同的是汇聚交换机旁挂一台具有认证功能的交换机作为网关，在旁挂交换机上基于网关部署 Portal 认证，对接入的用户进行身份认证，隔离非法用户和不安全用户。

图3-37 汇聚层旁挂认证方案组网图



3.9 华为 eSight 企业运维解决方案

3.9.1 概述

eSight 是华为推出的新一代面向企业园区和分支网络的管理系统，实现对企业资源、业务、用户的统一管理以及智能联动。

eSight 支持对 IT&IP 以及第三方设备的统一管理，同时对网络流量、接入认证角色等进行智能分析，自动调整网络控制策略，全方位保证企业网络安全。同时 eSight 提供灵活的开放平台，为企业量身打造自己的智能管理系统提供基础。

针对企业网场景，华为 eSight 提供多种应用，包括：多厂商的设备管理；企业资源统一管理；可视化的企业统一视图；全方位的企业故障监控；机房精细化监控；辅助智能楼宇安防监控；企业网络监控性能管理；分权-分域-分时的用户管理。

- 多厂商的设备管理

  eSight 预集成业界主流设备，默认已包含 Cisco20 个系列 140 余款设备、H3C14 个系列 130 余款设备、其他厂商 100 余款设备、以及数十款打印机、服务器。企业运维人员不做任何配置，即可管理全网设备，大大提升管理效率。

eSight 拥有厂商新款设备自动配套能力，通过 eSight 厂商类型自动识别能力，对于友商新发布的设备也可实现拓扑、告警、性能等管理能力。

针对业界主流设备深入分析，不仅支持标准的流量采集，还同时支持设备面板、设备 CPU 利用率等私有属性的管理。

- 企业资源统一管理

  如图 3-38 所示，华为 eSight 提供全方位的企业资源管理，针对不同网络设备、不同业务、不同服务器、工作站等 PC 资源进行管理。

图3-38 企业资源统一管理示意图

- 可视化的企业统一视图

  IP 网络是开放的，各厂商混合组网成为企业组网普遍情况。大部分企业不会像运营商一样建设综合网管，新厂商进入导致企业运维人员将面对多套厂商管理系统分而治之的情况。如果不具备全网设备统一监控的能力，出现网络故障后需要登录到多个网管查看状态，会导致管理效率低下。

  eSight 预集成业界主流设备，默认已包含 Cisco20 个系列 140 余款设备、H3C14 个系列 130 余款设备、其他厂商 100 余款设备、以及数十款打印机、服务器。企业运维人员不做任何配置，即可管理全网设备，大大提升了管理效率。

  eSight 拥有厂商新款设备自动配套能力，通过 eSight 厂商类型自动识别能力，对于友商新发布的设备也可实现拓扑、告警、性能等管理能力。

  - 自动发现：自动发现网络资源，网络链路自动创建。
  - 统一视图：提供 IT&IP 一体化拓扑视图，全面管理企业资源。
  - 实时呈现：呈现子图、网元、链路、网元状态，实时了解网络的运行情况。
  - 灵活定义：按用户信息保存网元位置，支持拓扑背景图和自定义图标功能。各种 Tips 信息，企业结构一目了然。

  针对业界主流设备深入分析，不仅支持标准的流量采集，还同时支持设备面板、设备 CPU 利用率等私有属性的管理。

- 全方位的企业故障监控

华为 eSight 提供全方位的故障监控，提供包括基于 IP 设备、基于 IT 设备、基于业务应用等丰富的告警，同时提供 7*24 不间断的故障监控，实时故障提醒和实时故障远程通知，同时也能提供丰富的故障统计功能。

- 机房精细化监控

  传统用户机房的设备管理都是亡羊补牢型的，如：设备高温烧毁了才发现网络故障；电源坏了才赶去维修。

  而如果能够在温度或电源发生异常时就及时知会网络管理员，就会避免最终设备失效带来的长时间断网以及重大维修。

  电力不稳地区，设备突然掉电重启，管理员无法判断具体原因。设备掉电前瞬间如果能上报网管掉电，则可以使网络管理员及时处理。

  华为 eSight 解决方案，通过引入 S3700-28TP-EI-MC 盒式交换机，支持环境监控口，支持 4 路信号输入和 3 路信号输出，实现机房环境在网络平台上的统一监控，提前对异常进行感知并上报网管，同时根据需要进行声光告警。如与接入网 E 系列机柜一起实现可以实现机柜门、温度、湿度的告警监控。

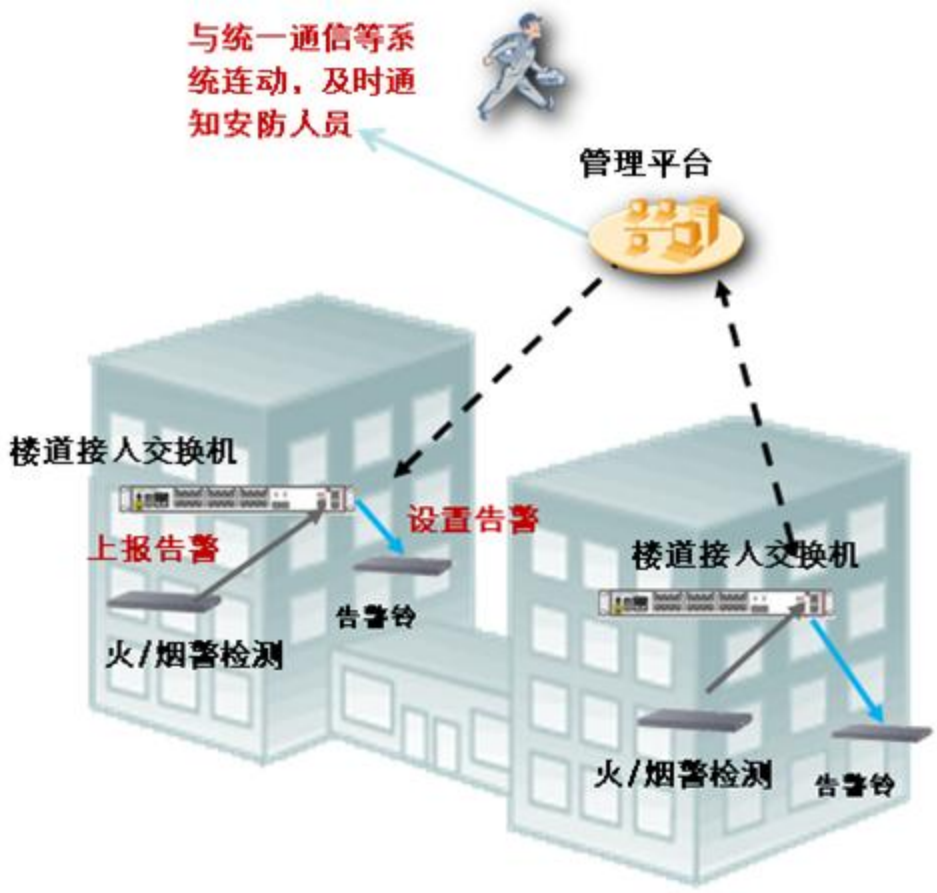
  Dyinggasp 功能（S3700-28TP-EI-MC 和 S5700-6TP-LI）实现断电瞬间告警发送，通知管理员设备复位是由于供电异常所致。

- 辅助智能楼宇安防监控

  智能楼宇建设中，对火警、盗警等安防检测主要是通常的闪灯、声音报警等手段，如何能够将各种报警信息汇总到统一管理平台，以便进行灵活处理？华为 eSight 通过网络设备监控口，实现安防告警信息 IP 化，灵活处理告警。在触发声光告警的同时，短信及时通知安防人员。

  还支持与 IP 视频监控联动，实现统一安防。网络管理平台通过上报告警的网络设备判断告警位置，切换视频监控查看现场状态，指挥救援。

图3-39 辅助智能楼宇安防监控示意图



- 企业网络监控性能管理能力

  华为 eSight 提供强大的企业网络监控管理能力、提供图形方式呈现性能数据，可以直观了解企业设备、服务器等资源设备性能情况；提供性能阈值告警能力，可以对企业网络健康度实时了解，保障企业业务承载网络健康性；自动创建设备基本性能监控；支持批量创建同类性能监控实例，方便客户轻松操作。

- 分权-分域-分时的用户管理

  为不同用户分配不同权限，并记录操作日志；设置用户管理区域；限定用户管理范围；限定用户帐户有效时间、有效期。

3.9.2 网络日常维护场景

日常维护概述

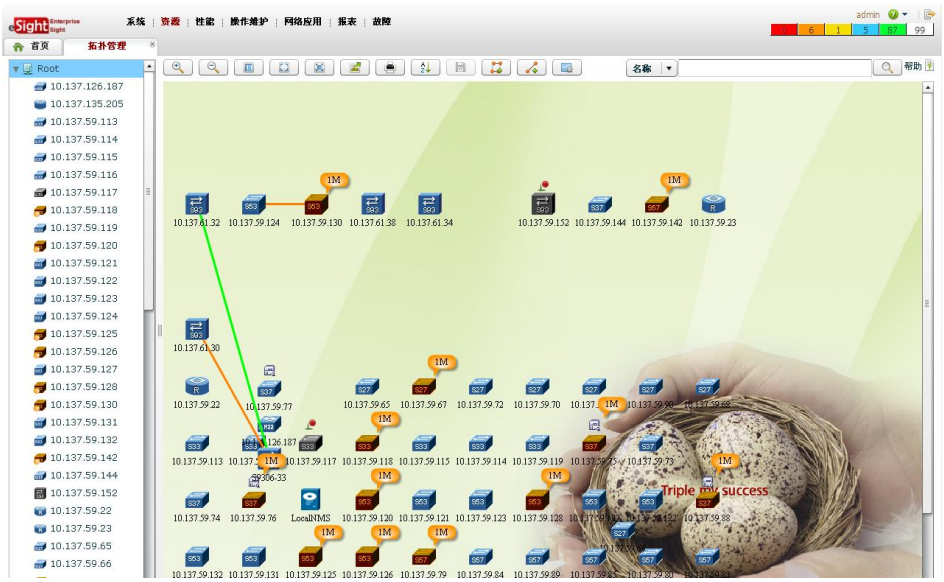
对于网络运维人员而言，日常维护工作不仅繁杂，而且工作量大，涉及的工作内容包括监控拓扑对象、监控网元、配置网元、监控业务、诊断故障、监控性能、查看资源、报表生成等。

华为公司推荐 eSight 网络管理系统，可以准确、快捷的提供运维人员所需要的信息，大大减轻运维人员的工作量。通过 eSight 网络管理系统丰富的管理功能和灵活多样的维护手段，可以轻松实现网络日常维护。

拓扑管理

如图 3-40 所示，eSight 以左树右图的方式组织整个视图，其中左边导航树以树型直观的体现出网络结构的层次关系。右视图在背景图上将指定网络层次的对象显示在不同的坐标上，可直观了解对象部署。

图3-40 监控TOPO对象



eSight 的拓扑图提供以下功能：

- 支持对拓扑上子网、网元、链路、虚拟网元等的增、删、改、查。
- 支持移动拓扑上的元素。
- 支持显示告警状态及 Tips 信息。
- 支持排列、浏览属性、放大缩小、打印等常用基本操作。
- 支持在拓扑图中提供其他功能的快捷操作入口，如：进入网元管理器查看设备相关告警等。

eSight 的拓扑告警提供以下功能：

- 支持通过拓扑节点的颜色监控设备的轮询状态（正常、未知、离线等）。
- 支持屏蔽显示低级别告警，当网元或子网同时产生多条告警时，系统只显示最高级别告警。

网元监控

网元管理器首页提供设备基本信息、TOPN 告警、接口流量、带宽利用率、CPU、内存等性能图表，用户可进行定制是否显示各图表。

图3-41 网元管理

eSight 针对各种不同类型的设备，支持丰富的网元监控和管理功能，如表 3-7 所示。

表3-7 eSight 网元监控功能

设备类型	支持的功能
华为路由器、交换机	提供完整的性能采集、告警监控能力。 提供设备基本信息管理功能。 支持通过适用仿真图片的设备面板查看设备状态，并支持单板、端口状态的联动显示。 支持查看设备的接口数据、IP 地址数据。 支持单网元的配置管理功能。 提供设备配置文件的查看、备份、恢复、比较的功能。 提供设备、机框、单板、子卡、端口的资源管理功能。
华为防火墙	提供基于标准实现的性能采集、告警监控能力。 提供设备基本信息管理功能。 支持通过仿真图片的设备面板查看设备状态，并支持单板、端口状态的联动显示。 支持查看设备的接口数据、IP 地址数据。 支持调用设备的 Web 网管提供单网元的配置管理功能。 提供对设备配置文件的查看、备份、恢复、比较的功能。

设备类型	支持的功能
预集成的主流CISCO、H3C设备	提供基于标准实现的性能采集、告警监控能力。 提供设备基本信息管理功能。 支持通过使用仿真图片的设备面板查看设备状态，并支持单板、端口状态的联动显示。 支持查看设备的接口数据、IP 地址数据。 支持调用设备的 Web 网管提供单网元的配置管理功能。 提供应设备配置文件的查看、备份、恢复、比较的功能。 提供设备、机框、单板、子卡、端口的资源管理功能。
未预集成的第三方设备	提供基于标准实现的性能采集、告警监控能力。 提供设备基本信息管理功能。 支持通过基本图片查看设备面板，基于设备定制提供单板、端口状态的联动显示。 基于设备定制功能，用户可以通过输入定制数据实现并支持设备图标展示、设备自身的性能采集、告警上报、配置文件备份。
服务器、打印机	提供基于标准实现的性能采集能力。 提供设备基本信息管理功能，例如设备基本属性。 支持通过使用仿真图片的设备面板查看设备状态，并支持单板、端口状态的联动显示。 支持查看设备的接口数据、IP 地址数据。 支持调用设备的 Web 网管提供单网元的配置管理功能。 提供服务器、打印机的设备存量管理功能。

配置网元

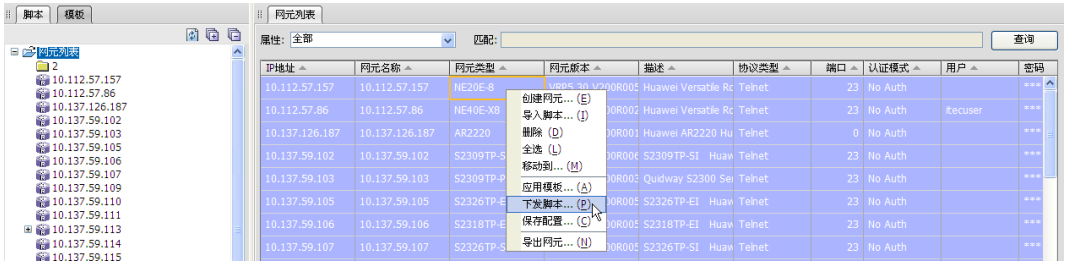
eSight 网络管理系统可以通过三种方式完成单点网元配置工作：

- 使用简单配置框架实现单点网元配置。
- 使用智能配置工具进行设备单点配置。
- 通过 Web 网管进行单点配置。

在开局、网络维护等多个场景，用户有对集中部署的设备的业务进行批量操作的需求，如图 3-42 和图 3-43 所示，用户通过智能配置工具能够对多台设备的业务进行批量配置，提高用户的运维效率。

图3-42 网元批量配置 1

图3-43 网元批量配置 2



监控业务

eSight 网络管理系统能够对业务进行实时监控，根据业务类型进行流量、信息统计，极大的方便网络运维人员实时监控业务状况。

监控性能

eSight 可以对网络的关键性能指标进行监控，并对采集到的性能数据进行统计。通过可视化的操作界面，方便用户对网络性能进行管理。

通过监视模板管理性能监视指标，并设定告警的阈值。通过性能监视模板，用户可以方便的将性能采集规则应用到多个对象中。性能监视模板包括以下内容：

- 性能指标组

  将多种性能指标集成到一个性能指标组中，可以支持分场景定制指标组，包含场景相关的所有性能指标，便于根据业务场景建立对应的监视任务。

- 性能指标

  定义具体的性能采集的指标。

- 采集周期

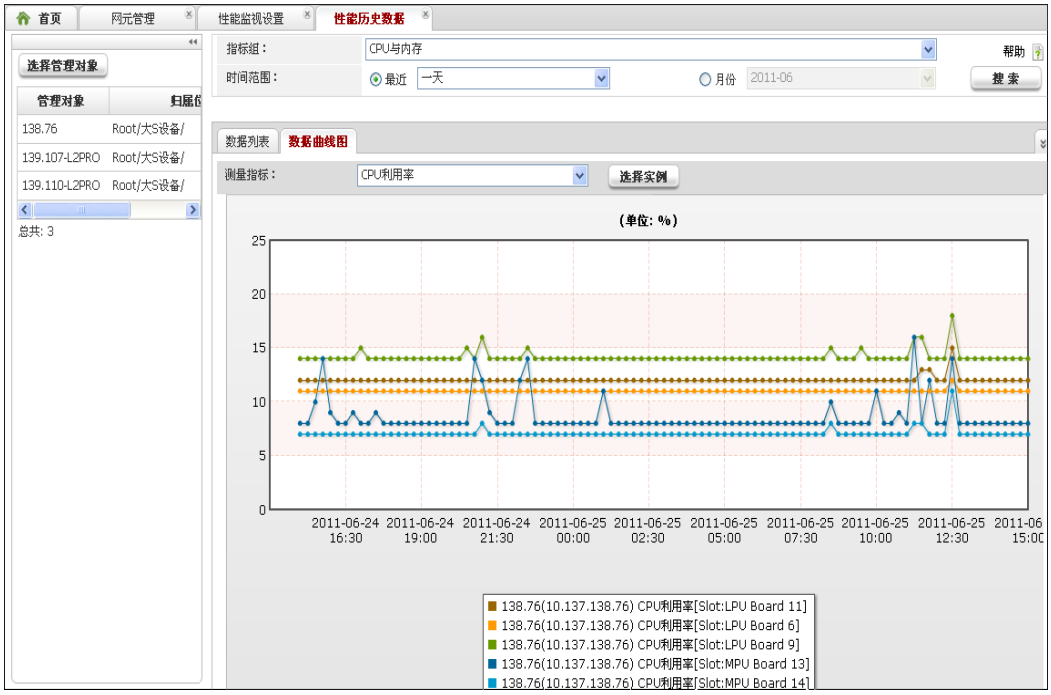
  提供多种采集周期供采集性能指标时选择。

- 性能阈值

  通过设置性能门限值，可以在网络的性能数据低于门限值时及时预警，避免网络性能的持续恶化。

通过性能监视的设置，实现网络性能数据的采集。支持周期性性能指标采集，可以了解网络在指定时间范围内的性能状况，并为预测网络的性能变化提供数据依据。如图 3-44 所示。

图3-44 性能监控



通过性能监视设置获取网络性能数据后，可以通过性能监视视图以图形化的方式进行指标值查看。用户可以了解网络在指定时间范围内的性能状况，为预测网络的性能变化提供数据依据。

资源查看和报表管理

eSight 提供丰富的资源查看和预定义报表，同时提供强大易用的报表设计功能，用户可根据行业特点和自身运维要求进行客户报表定制。如图 3-45 和图 3-46 所示。

图3-45 查看物理资源

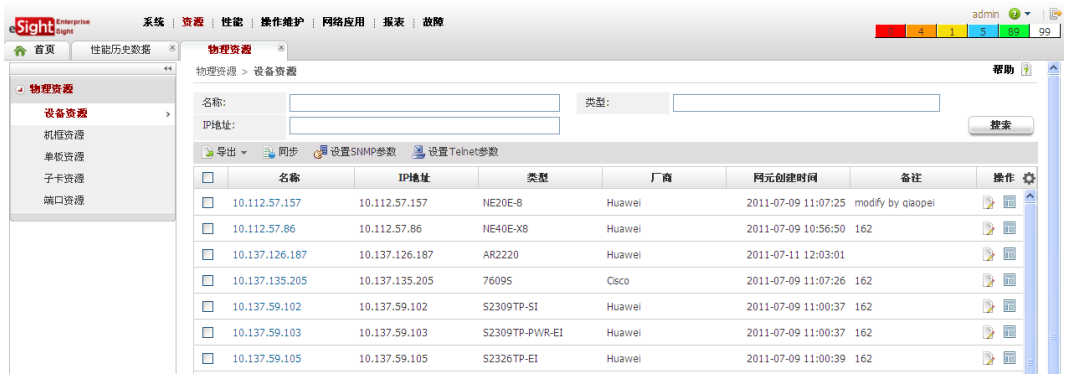
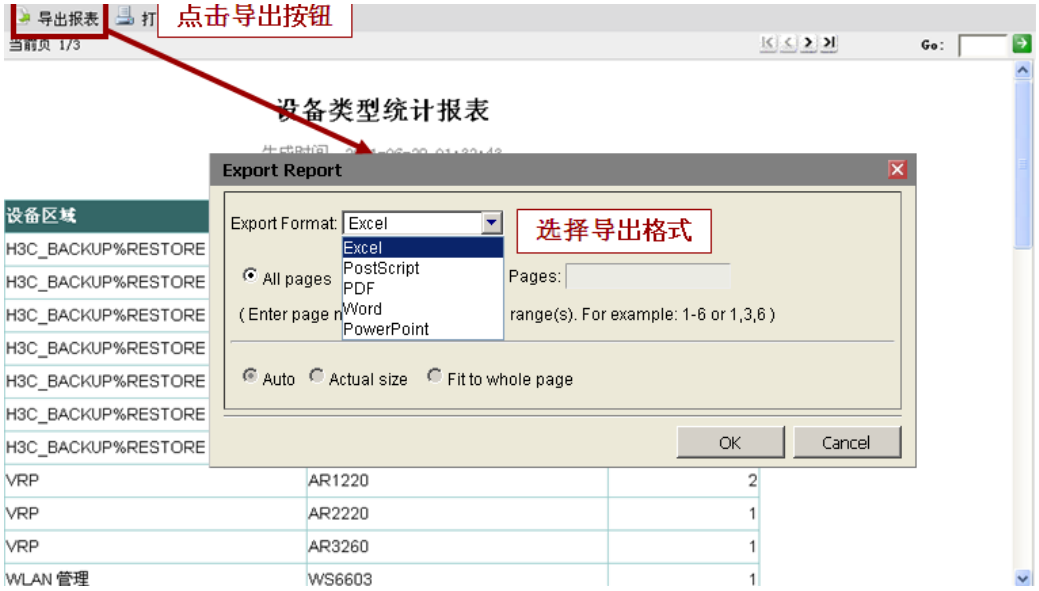


图3-46 导出报表



阶段维护

eSight 提供配置文件管理和备份功能，可以快速的进行文件备份和设备登录管理。同时还提供系统巡检工具，能够定时对设备进行自检，减轻网络维护人员的工作量。

3.9.3 第三方设备定制场景

园区网络设备来自不同厂商，无法统一采用预集成的方式管理第三方设备，需要提供定制的能力。如果使用各自的网管系统进行管理，不仅增加了运维成本，而且极大的增加了网络维护人员的工作量。

华为公司 eSight 网管系统提供了对第三方设备管理能力的定制功能，包括对设备厂商信息、设备型号信息、告警参数、性能指标、设备面板、设备配置文件管理的定制功能，方便用户实际网络设备进行定制化的管理。满足对第三方设备的管理需求。

- 厂商信息定制

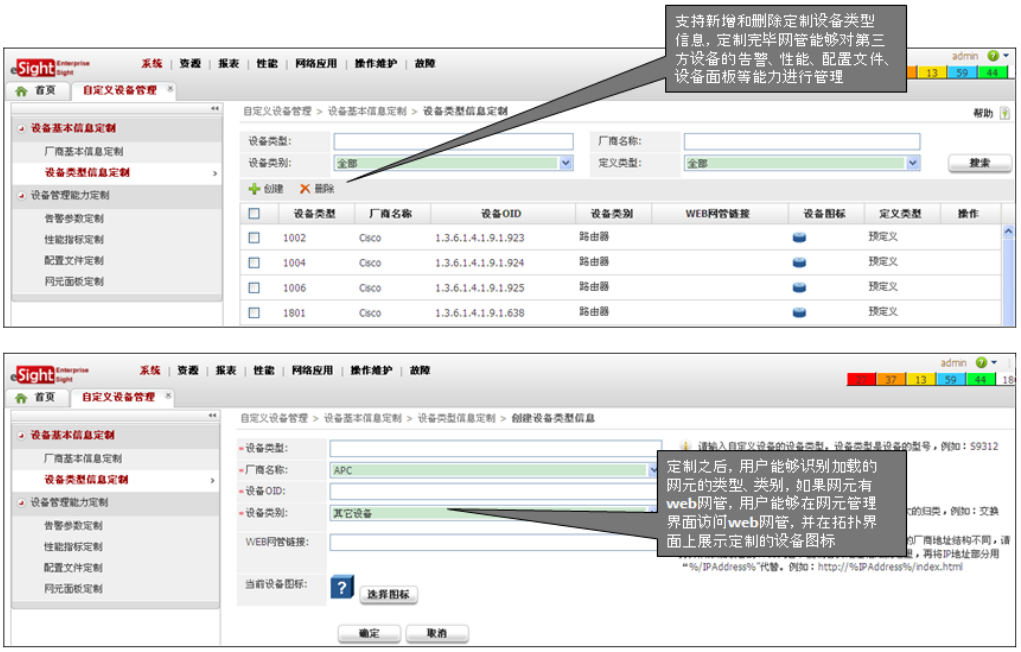
  eSight 网管系统可以定制厂商的名称、联系人等信息，用于后续的设备类型定制。如图 3-47 所示。

图3-47 厂商信息定制

- 设备类型定制

  eSight 网管系统可以定制设备类型的描述、设备图标、Web 网管链接信息，定制的设备图标能在拓扑上显示。如图 3-48 所示。

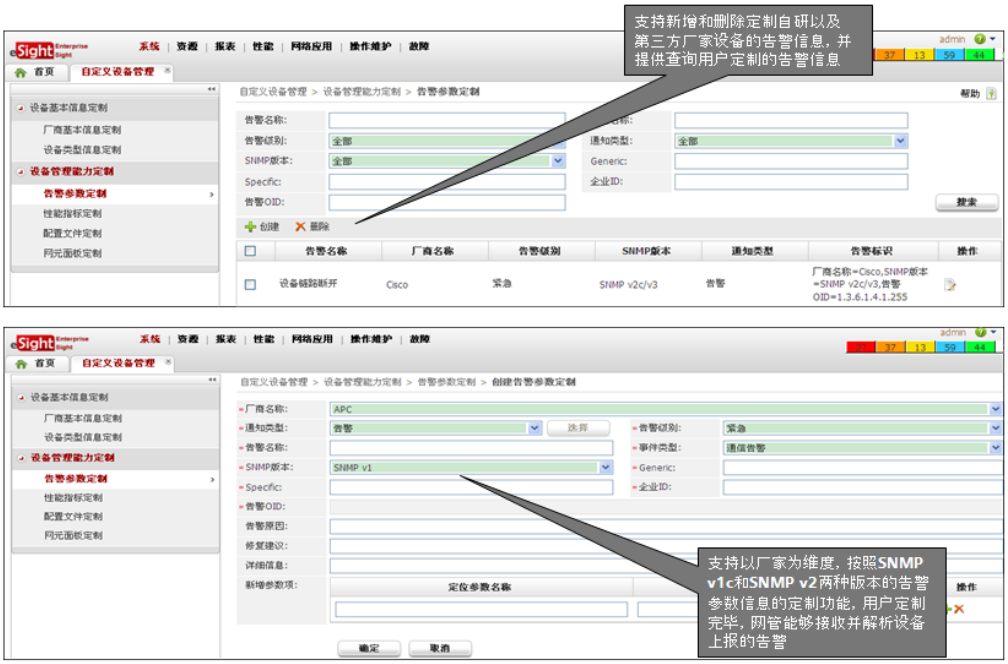
图3-48 设备类型定制



- 告警定制

eSight 网管系统可以对上报告警格式进行定制，定制后的告警能支持告警报文解析，并在告警管理界面上进行显示。如图 3-49 所示。

图3-49 告警定制



- 性能指标定制

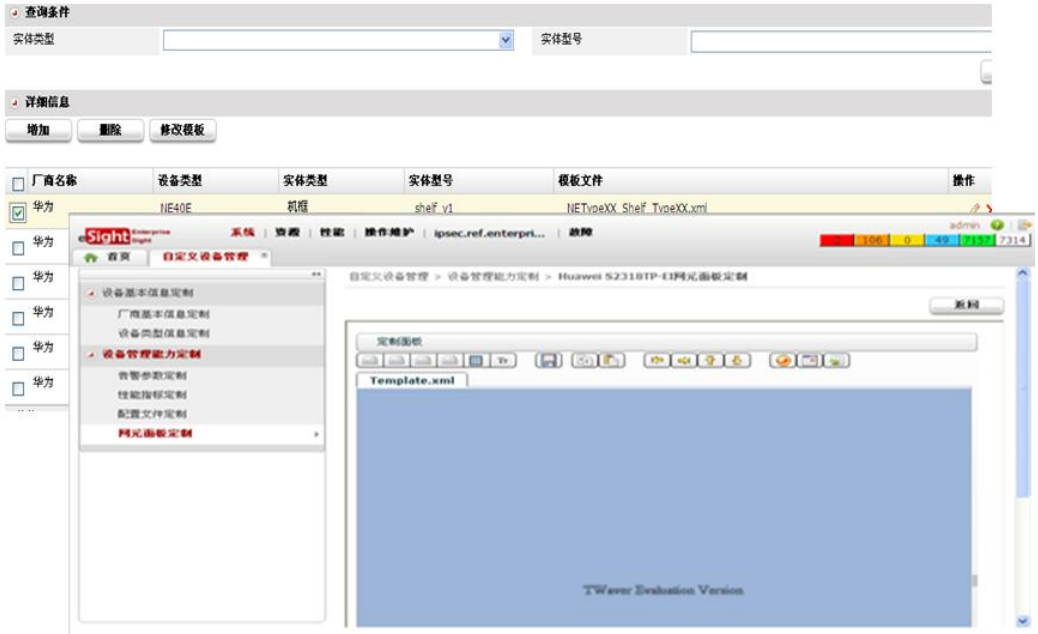
  eSight 网管系统可以对设备上支持的采集指标进行定制，定制后的性能指标能通过性能任务进行采集，在性能界面中进行数据浏览。如图 3-50 所示。

图3-50 性能指标定制

- 设备面板定制

  eSight 网管系统可以对设备框、单板、子卡、端口进行仿真图定制，定制后的面板将显示新的仿真图。如图 3-51 所示。

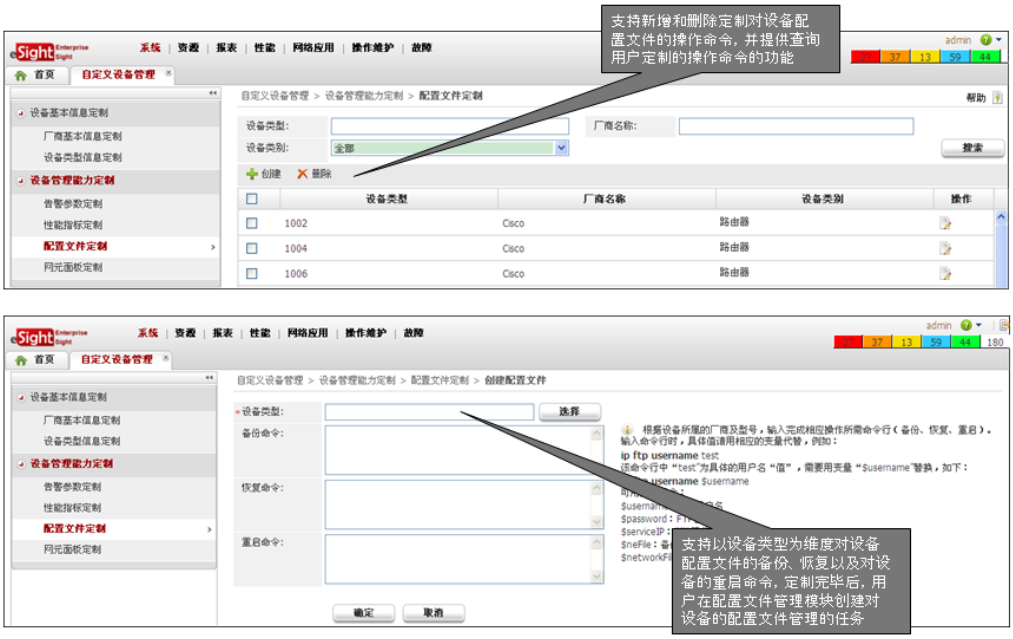
图3-51 设备面板定制



- 设备配置文件定制

  eSight 网管系统可以针对第三方设备定制关于配置文件的备份、恢复、重启命令，支持配置文件自动备份。如图 3-52 所示。

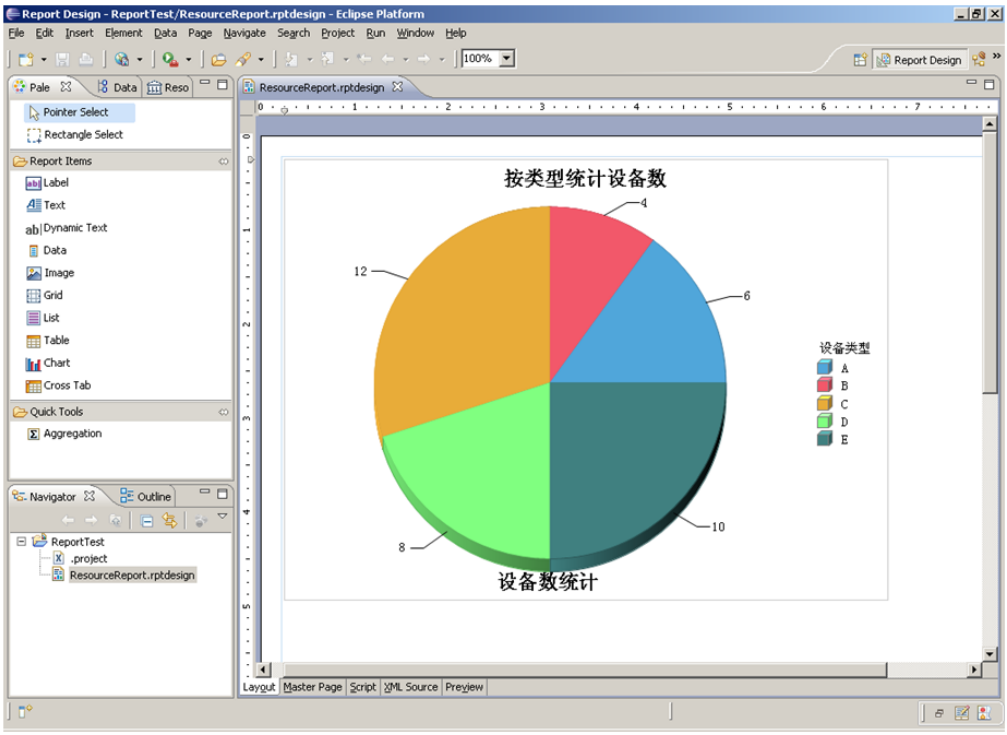
图3-52 配置文件备份和恢复定制



- 报表定制

  eSight 提供强大的自定义报表能力。提供所见即所得的报表设计环境，可以修改现有的报表设计文件，生成新的设计文件。如图 3-53 所示。

图3-53 报表定制



3.9.4 软件升级和补丁加载场景

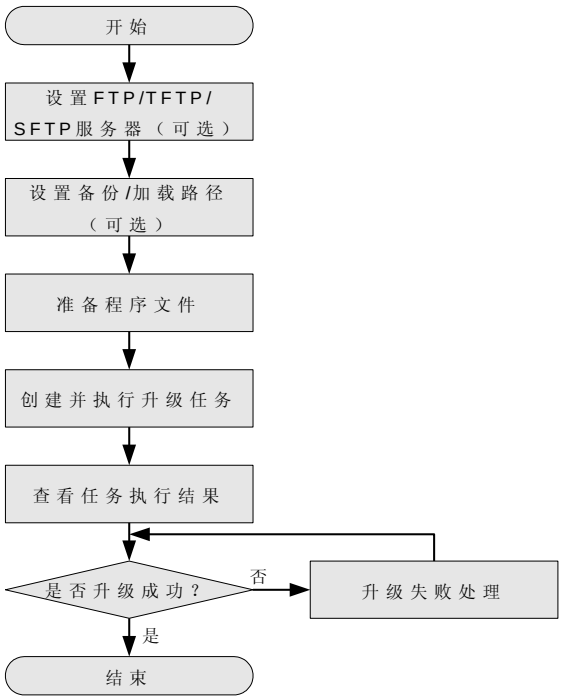
园区网络设备众多，如果使用一台一台的方式去升级和加载补丁，不仅耗时耗力，而且容易出现人为原因造成的升级失败，需要考虑通过远程集中式进行统一升级和加载补丁。

eSight 网管系统提供了远程集中式软件升级和补丁加载机制，极大的减轻网络维护人员工作量，避免了人为原因造成的升级失败和补丁加载失败。

- 软件升级

  eSight 网管系统提供远程集中式的软件升级功能，按照操作向导，轻松完成设备升级，并且对升级失败有相应的处理，避免升级失败后的设备状态异常。如图 3-54 所示。

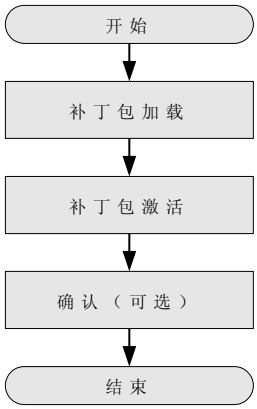
图3-54 软件升级流程



- 补丁加载

  eSight 网管系统提供远程集中式的补丁加载功能，按照操作向导，轻松完成补丁加载，并且具有补丁回滚功能，可以将网元恢复到补丁升级前的状态。如图 3-55 所示。

图3-55 补丁升级流程



3.9.5 故障处理

园区网络系统是由网络设备、连接设备间链路和一些相关服务器组成。因此出现网络系统故障的原因也基本上从链路、网络设备状态、是否受病毒攻击、服务器状态等方面来查找。这些组件的任何一个出现故障，都会导致上层应用无法正常工作。

3.9.6 网络设备故障处理

网络设备发生故障可以分为几种：

- 设备宕机：设备上的电源或者其他指示灯都不亮，没有任何工作时的声响。
- 设备 CPU 使用率高：监控软件或者登录设备时，发现设备的 CPU 利用率很高，同时相关应用响应较慢。
- 有错误消息：查看日志服务器或者登录设备时，发现设备有错误消息。
- 有报警信息：设备状态指示灯报警，显示为红色等。

针对以上几种设备故障，可以做如下处理：

- 设备宕机

  如果发现一旦发现设备宕机，首先检查电源连接线和机房电源。如果电源连接线和电源均正常，立即拨打设备提供商和服务提供商的服务号码，请求支持。如果发现设备硬件存在问题，可要求设备提供商和服务提供商在最短时间内做备件更换服务。
- 设备 CPU 利用率高

  立即报告服务提供商，要求提供技术支持。待技术支持工程师远程处理或到场后，协助工程师找出设备 CPU 利用率高的原因。一般情况下，可以判断为设备受到病毒的攻击。
- 有错误消息

  将错误消息发送给服务提供商，并跟踪进度。经过服务提供商分析后，给出错误消息的原因，如果设备有隐形的故障，可以预先做好相应的准备工作或者更换设备。
- 报警信息

  报告服务提供商和设备提供商，要求对设备进行报警故障排除或者更换硬件。

3.9.7 服务器故障处理

跟网络系统相关的服务器主要有 DHCP 服务器、ACS 服务器、外网代理服务等。常见的故障现象包括：

- 不能正确获取 IP 地址。
- 不能正常登录网络设备。
- 不能通过代理服务器上网。

可以按照如下步骤进行故障处理：

- 不能正确获取 IP 地址
  - 首先查看 DHCP 服务器的连通性，可以用 Ping 的办法确定。如果 DHCP 服务器连通性正常，则可以登录服务器。
  - 查看该服务器的 DHCP 服务是否正常；如果服务正常，可以查看是否网络当中有病毒，导致 DHCP 的请求消息超时。
  - DHCP 服务器有备份服务器，在当前服务器不可用的情况下，可以替换当前的服务器。
  - 在 DHCP 服务器恢复正常工作前，我们也可以采用手动静态配置 IP 地址的方法来临时解决电脑访问网络的问题。

- 不能正常登录网路设备
  - 首先查看该网络设备是否具有连通性。
  - 如果该设备可以 Ping 通，可以尝试登录服务器，看 ACS 的服务器的服务是否正常。
  - 如果服务不正常，可以考虑使用网络设备上的 Console 端口登录设备，临时去掉 AAA 认证服务相关配置，启用网络设备的内置本地认证数据库进行临时登录认证。
- 不能通过代理服务器上网
  - 首先查看网络是否连通，是否可以访问其他的应用；然后测试到代理服务器的连通性。
  - 如果代理服务器连通性正常，则可以登录服务器，查看该服务器的代理服务和相关系统服务是否正常。如果发现服务不正常的，可以尝试重启服务或者服务器来解决。
  - 如果重启代理服务器服务或系统后问题仍无法解决的，则需进一步检查代理服务器硬件是否存在故障，例如网卡等关键硬件。
  - 如果代理服务器硬件或者系统存在问题的，我们可以临时使用备用代理服务器来满足代理上网的需求。
  - 如果前述问题均不存在，一切正常，则可以测试到 Internet 的访问是否正常。我们应该对提供 Internet 服务的 DNS 和 ISP 网关进行 Ping 测试。如果 DNS 或 ISP 网关存在连通性问题，则及时联系 ISP 商排查解决。对于 ISP 提供的当前线路出现问题的，我们可以使用备份线路进行 Internet 访问。

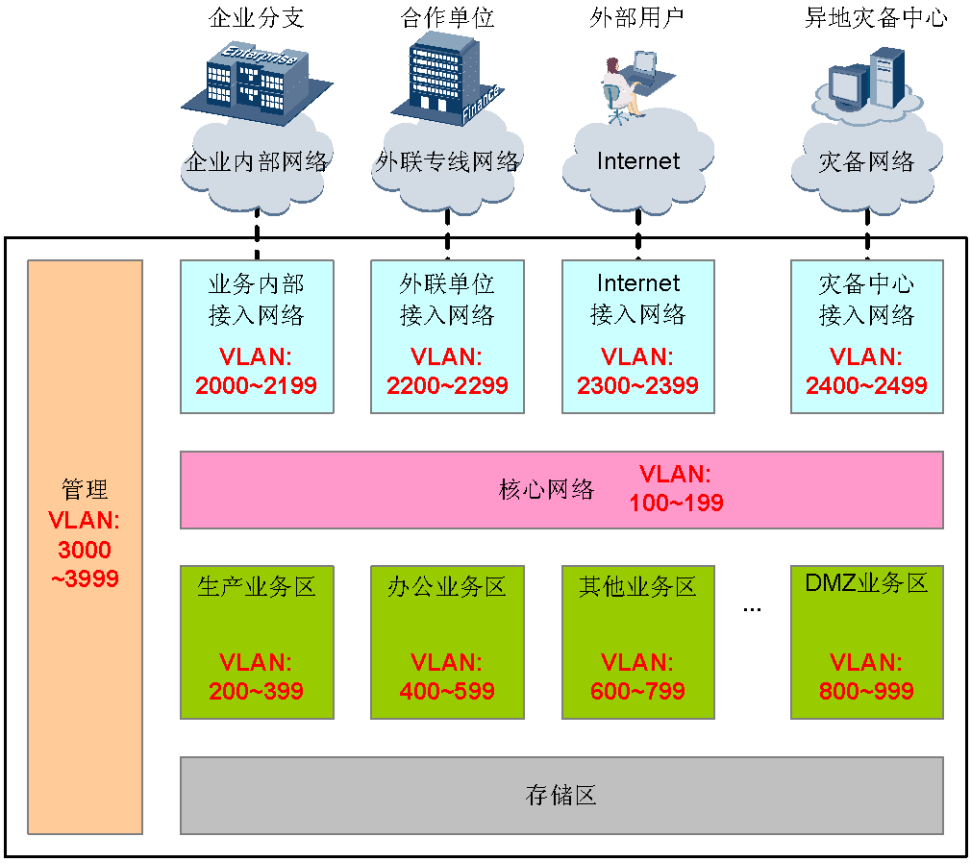
3.9.8 网络扩容

随着园区网络业务、规模的不断增加，现有网络容量已经不能满足园区网络的长期发展，在不影响现有业务的情况下实现平滑扩容，是园区网络扩容的基本要求。

服务器扩容

服务器扩容包含在原区域扩容服务器和在新区域新建服务器两种情况，针对这两种情况，所采取的扩容策略不尽相同。

图3-56 园区网络内部架构



- 原区域扩容服务器

  随着生产业务的不断发展，当前生产业务区的服务器资源已经不能满足业务发展需要，需要进行生产业务区服务器的扩容，实现平滑扩容需要使用该区域初期规划好的 VLAN，保持 VLAN 的连续性，并且 IP 地址使用该区域初期规划好的地址段，这样做可以保证上游路由和防火墙策略不需要进行修正，便于维护的同时也减轻了扩容工作量。

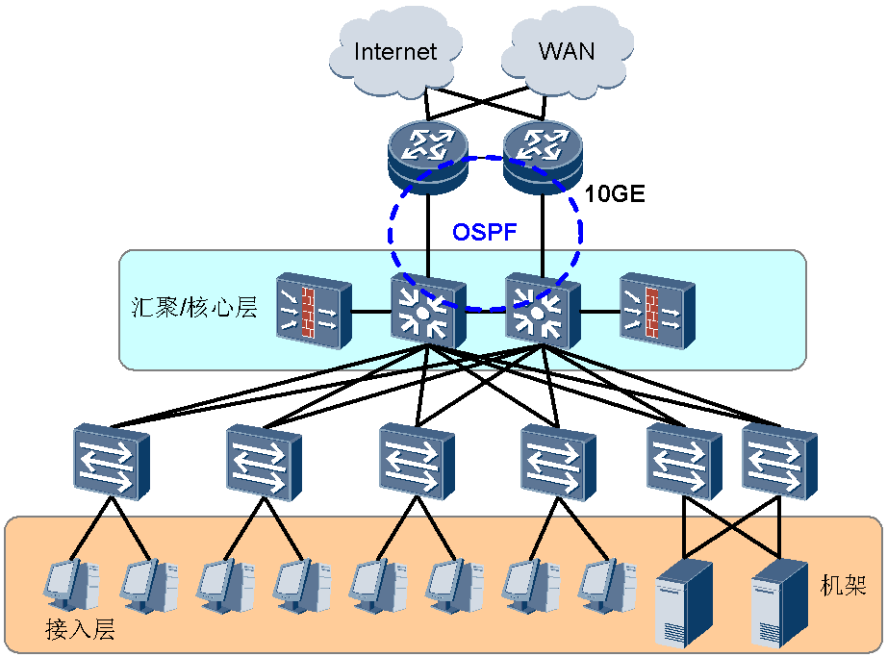
- 新区域新建服务器

  假设 DMZ 区是新建区域，那么就需要为该区域重新规划 VLAN 资源和 IP 地址资源，重新进行路由和防火墙策略规划，这样做可以确保新区域的建设不会影响到现有业务，实现现有业务的平滑扩容，划分新的区域也便于今后运维管理。

网络设备扩容

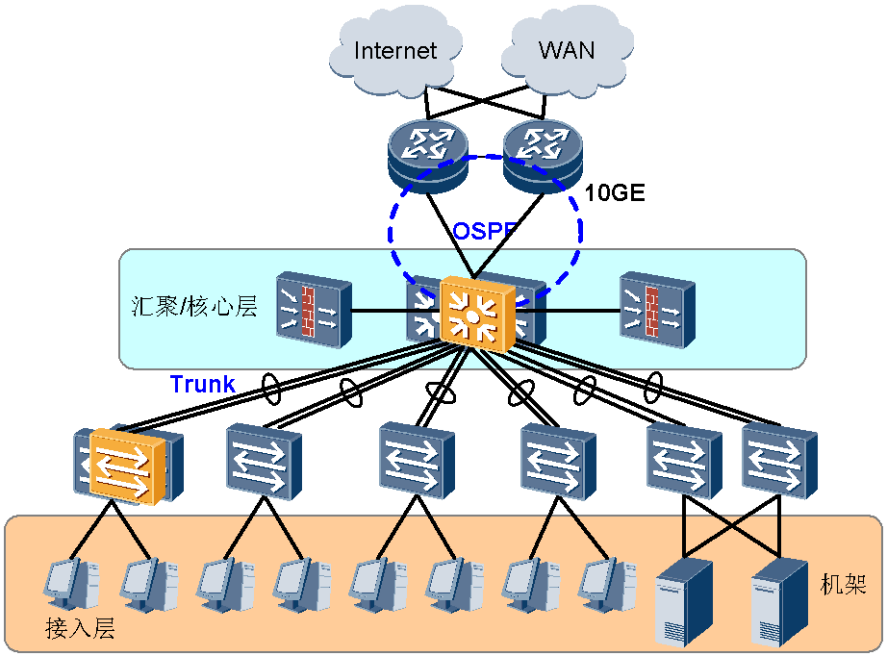
图 3-57 所示为通用的园区网络架构。可以看到在接入与汇聚层存在众多环网，一旦由于业务增长需要增加服务器资源，就需要增加接入层交换机并连接到汇聚/核心层，增加网络复杂度的前提下还要使用破环技术，不可避免的会对现网的业务产生影响。

图3-57 通用园区网络架构



华为公司推荐在园区网络架构采用堆叠和集群技术，首先消除破环协议，其次简化网络规模，并且利于网络设备扩容。如图 3-58 所示。

图3-58 堆叠/集群化的园区网络架构



使用堆叠和集群技术后，网络结构由环形简化为树形。首先利于网络运维管理，其次网络设备扩容时，只需要在原有的堆叠环境下新增设备，对网络结构不产生影响，也不需要添加物理链路到汇聚/核心层，实现园区业务的平滑扩容。

链路带宽扩容

随着园区业务的扩展，链路带宽也会成为园区业务的瓶颈，除了使用更换高性能、高带宽单板外，还可以通过链路捆绑技术进行链路带宽扩容，在不影响现网业务的情况下实现链路带宽的平滑扩容。

4 业务解决方案

4.1 虚拟园区网解决方案

4.1.1 虚拟园区概述

园区网通过在核心层、汇聚层以及接入层部署集群（CSS）、堆叠、Eth-Trunk 和 MPLS VPN 技术实现横向虚拟化和纵向虚拟化，解决传统企业网的二层环路和可靠性等问题，同时实现企业内部不同部门、不同业务的隔离。

网络中位于核心层和汇聚层的交换机使用集群技术解决单点故障问题，接入层采用堆叠技术解决环网的难题，抛弃了复杂的环网协议，简化网络，降低管理成本；堆叠、集群技术同时提供了冗余设计，可靠性得到大幅提升。

4.1.2 横向虚拟化

横向虚拟化即在园区网的核心层、汇聚层、接入层分别采用集群/堆叠技术，将多台物理设备虚拟化成单台逻辑设备，达到简化网络结构、简化网络协议部署、提高网络可靠性和可管理性的目的。

接入层在复杂的接入环境中运行堆叠技术，可以最多将 9 台物理网络节点虚拟化为单台设备，完全消除接入层环路，并形成捆绑链路的高带宽和可靠性上行。汇聚层与核心层一般是将两台设备组成集群环境，简化网络拓扑，提高带宽利用率。横向虚拟化可实现网络灵活扩展。

优点

横向虚拟化优点主要有：

- 部署简化

  在这样的虚拟化下，网状的企业园区网络形成了一个非常简洁的架构，网络各层之间通过捆绑的单逻辑链路互联，消除了环路。不再需要在接入层设计复杂的生成树协议，也不再需要在变成单一逻辑节点的客户端接入网关上运行 VRRP 协议。

- 路由简化

  端到端堆叠/集群部署，使园区网络形成了无环、树状、辐射型的网络拓扑结构，极大简化了运行维护工作。网络中数据流在宏观路径上与简化后的整体网络拓扑具有一致性，业务流在网络中的走向清晰明确。同时，每个堆叠/集群节点本身的扩

展（如：增加该节点设备）既不会改变企业网络的逻辑结构，也不会影响上下层网络的协议交互。

- 管理简化

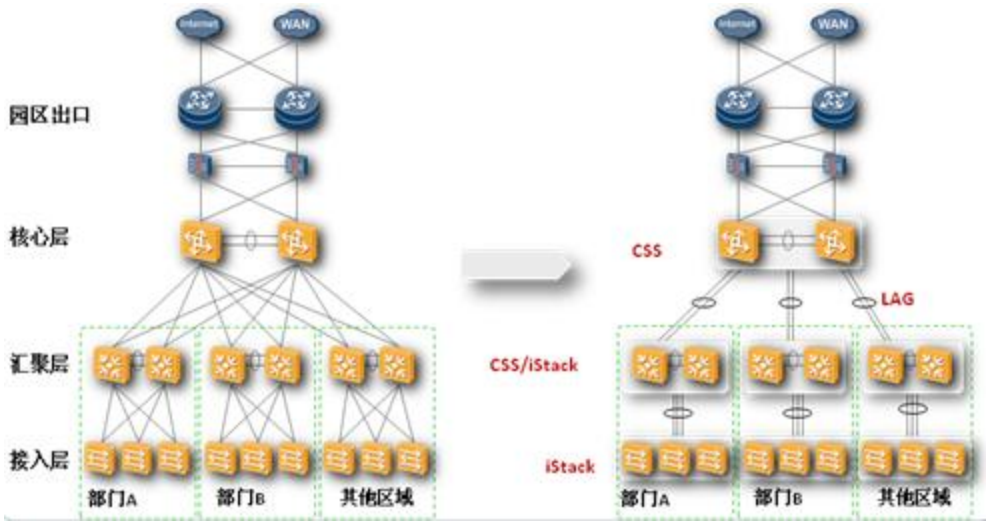
  横向整合后，原有的多台设备作为一台设备进行管理，对管理的设备的数量进行大大的简化，提高对设备管理的效率。

网络部署

横向虚拟化园区场景通过在核心层、汇聚层以及接入层部署集群、堆叠和 Eth-trunk 技术，解决传统企业网的二层环路和可靠性等问题。

- 在核心层采用集群(CSS) 技术，将多台核心交换机（推荐使用性能较高的 S97 系列）组合成一台逻辑设备，负责整个园区的互联。
- 在汇聚层和接入层，采用集群或者堆叠技术，将多台汇聚/接入交换机组合成一台虚拟的逻辑交换机；接入层是最靠近用户的网络，部署二层接入设备，汇聚层负责将大量用户接入互联网络，扩展核心层设备接入用户的数量。
- 在核心层、汇聚层和接入层之间，采用 Eth-trunk 技术，将多个物理接口捆绑在一起作为一个逻辑接口来增加带宽。

图4-1 堆叠/集群部署拓扑



如图 4-1 所示，在横向虚拟化园区场景下，通过在核心层、汇聚层和接入层部署集群和堆叠，将多台冗余设备虚拟化为单台逻辑设备。网状结构优化为简洁的树形结构，且能保证核心层、汇聚层和接入层的单设备出现故障时，不会导致大面积的网络瘫痪。

同时，通过各层间部署 Eth-trunk 技术，保证了在一条链路或者多条链路故障时，也不会引起网络瘫痪。横向虚拟化自然消除环路，无需再部署 MSTP 和 VRRP 等协议。

4.1.3 纵向虚拟化

纵向虚拟化就是把网络等硬件设备和应用服务等都看成统一的资源，通过技术手段和方案设计，把这套共有的资源虚拟成多套逻辑资源，供不同的群组或业务使用。虽然在物

理上这些资源是统一、集中的，但对不同的用户/业务来说，能够使用到的资源、配置的安全策略、配置的管理策略可能各不相同。

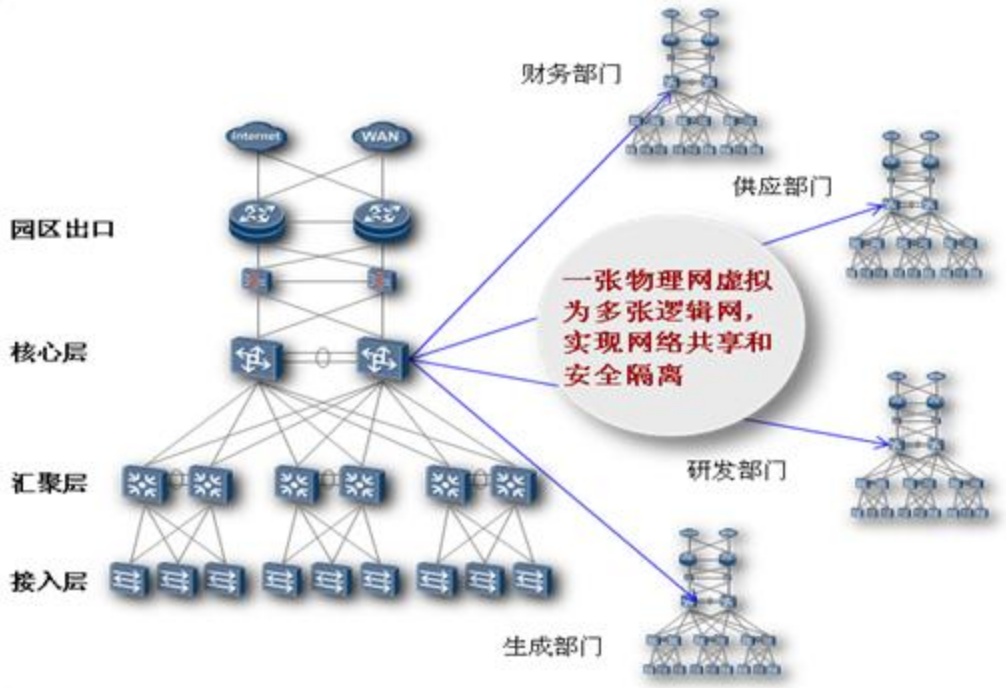
企业网的纵向虚拟化是指对企业网络中物理网络的逻辑虚拟化，即将一个物理网络虚拟为若干逻辑网络，且这些虚拟化的逻辑网络是相互独立的。

例如：一个园区网中有财务、供应、研发和生产四个部门，这些部门的纵向独立性要求其业务数据与其他部门的业务安全隔离，但协同办公又需要各部门业务能进行可控互访；园区内数据中心的部分服务器同时为多个部门提供服务、部分服务器只为某个部门内部提供服务。

这些复杂的需求使得传统的网络物理隔离方案已无法满足这些应用的需求。网络重复建设、分散管理、安全策略难部署、无法提供统一的应用服务等，都大大增加了用户在网络投资、建设、运维、管理方面的负担。

因此，我们需要一个便于扩展的解决方案，来保持用户群组的完全隔离，实现服务和安全策略的集中，并保留原有设计的高可用性、安全性和可扩展性的优势。通过将现有园区网络进行纵向的路径虚拟化很好地解决了这个问题，如图 4-2 所示。

图4-2 纵向虚拟化拓扑

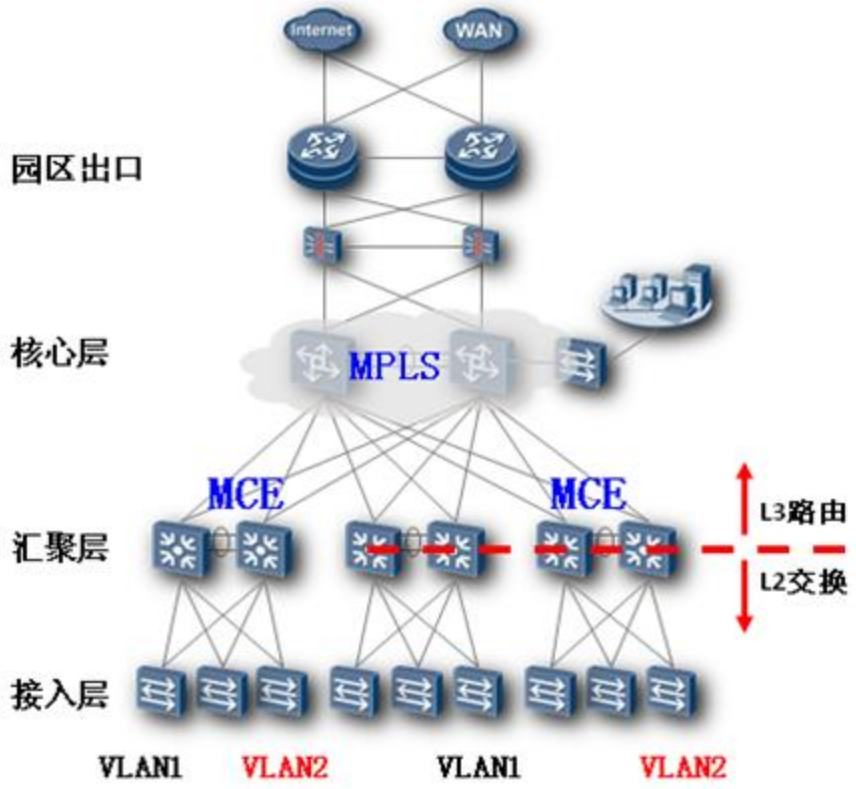


园区网络中不同层次的网络设备支持网络虚拟化所采用的技术手段也是不同的：

- 核心层的纵向虚拟化，主要采用 MPLS VPN 的方式，当然也可以使用 MCE，但是不建议使用 MCE，因为配置复杂，无法互通。
- 汇聚层的纵向虚拟化，可以采用 MPLS VPN，当汇聚层设备不支持 MPLS VPN 的时候，MCE 也是一种不错的选择，特别在配合核心层使用 MPLS VPN 的时候。
- 接入层的纵向虚拟化，当接入网络是二层网络时，采用 VLAN，当接入网络是三层网络时，采用 MCE。

这样，我们就可以看到一个纵向的虚拟化网络部署示意图了，如图 4-3 所示。

图4-3 纵向虚拟园区特性部署图



4.1.4 业务逻辑隔离规划

业务隔离概述

园区网络是企业办公业务、生产业务、销售业务的承载体，一方面企业对园区网络的可靠性、安全性、扩展性、高性能需求日益提高；另一方面，企业内部部门出于业务安全隔离的考虑，需要限制不同部门之间的业务互访，控制部门的资源访问权限。

传统的物理隔离方式将网络一分为多，需要隔离的业务独立占用一张网络，多张网络之间没有物理连接。传统的物理隔离方式势必造成网络资源、服务器资源的分散投资，网络的物理独立也增加了统一管理的难度。传统物理隔离方式部署昂贵，难以维护管理。这些致命缺点已使传统的物理隔离方式无法适应当下企业园区网络对高可用性、高可扩展性、统一维护管理的需求。

采用逻辑隔离方式，可以在统一的网络承载平台上，实现不同部门之间业务的安全隔离。逻辑隔离方式区别于传统物理隔离方式，主要采用 VLAN、ACL、VPN 等技术，从逻辑上对网络资源进行隔离区分。逻辑隔离方式不但简化了网络的复杂性和维护规模，而且从业务的角度看，网络层次明显，结构清晰，维护简便。

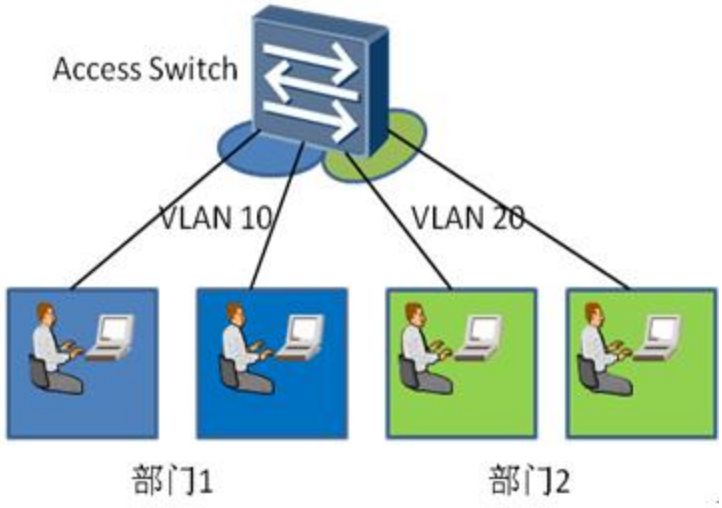
对园区内共用一个物理网络传输各种应用数据的逻辑隔离需求，华为提供了适合小型园区和大中型园区网络设计的解决方案。

小型园区业务隔离设计

小型园区业务隔离设计采用 VLAN+ACL 隔离方式。

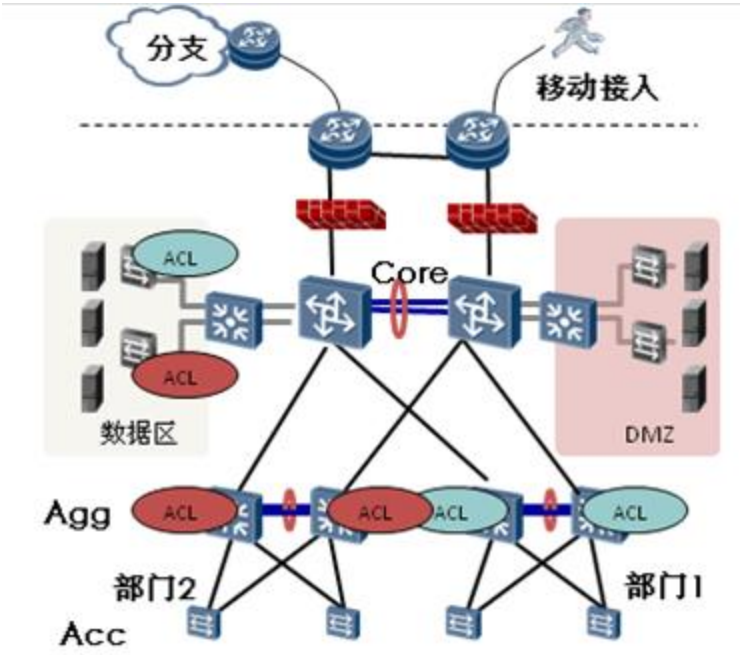
VLAN 是将一个物理的 LAN 在逻辑上划分成多个广播域（多个 VLAN）。同一 VLAN 内的主机间可以直接二层通信，而 VLAN 间不能直接互通。采用 VLAN，可以实现不同用户共享 LAN 设施，同时保证各自的网络二层隔离信息安全，如图 4-4 所示。

图4-4 二层网络 VLAN 隔离



VLAN 技术可以有效解决二层隔离的需求，而对于三层终结业务隔离则需要在网络三层边界和数据区边界部署 ACL，根据隔离要求设定策略控制，限制部门之间的访问权限，如图 4-5 所示。

图4-5 三层网络 ACL 隔离



采用 VLAN+ACL 方式隔离业务有如下特点：

- 部署简单，容易理解，特别适合小型园区网络。
- 采用 VLAN+ACL 实现业务隔离，对网络设备功能要求不高，有利于企业降低采购成本。
- 分布式 ACL 需要配置严格复杂策略控制，灵活性和扩展性较差。当业务、网络需要调整时配置需要跟随变动。

大中型园区业务隔离设计

MPLS L3VPN 是一种基于网络边缘设备 PE（Provider Edge）的 L3VPN 技术。它使用 BGP 在服务提供商骨干网上发布 VPN 路由，使用 MPLS 在服务提供商骨干网上转发 VPN 报文。

MPLS L3VPN 组网方式灵活、可扩展性好，并能够方便地支持 MPLS QoS 和 MPLS TE，因此得到越来越多的应用。从业务隔离的灵活性、配置复杂度、管理复杂度、扩展性、组网对设备的要求等多方面对比，MPLS L3VPN 技术最适合应用在大、中型园区内进行用户逻辑分组和业务隔离。

在大中型园区网络核心、汇聚、接入三层结构中，一般情况下汇聚交换机作为二三层网络分界点。MPLS VPN 都会从汇聚层部署，但是在汇聚层网络不支持 MPLS VPN 的时候，那么就只能在核心层部署了。在核心层部署 MPLS VPN 的时候，通常会在汇聚层部署 MCE 来配合完成隔离。

在汇聚层和核心层上部署 MPLS VPN 的示意图如图 4-6 和图 4-7 所示。

图4-6 汇聚层上部署 MPLS VPN

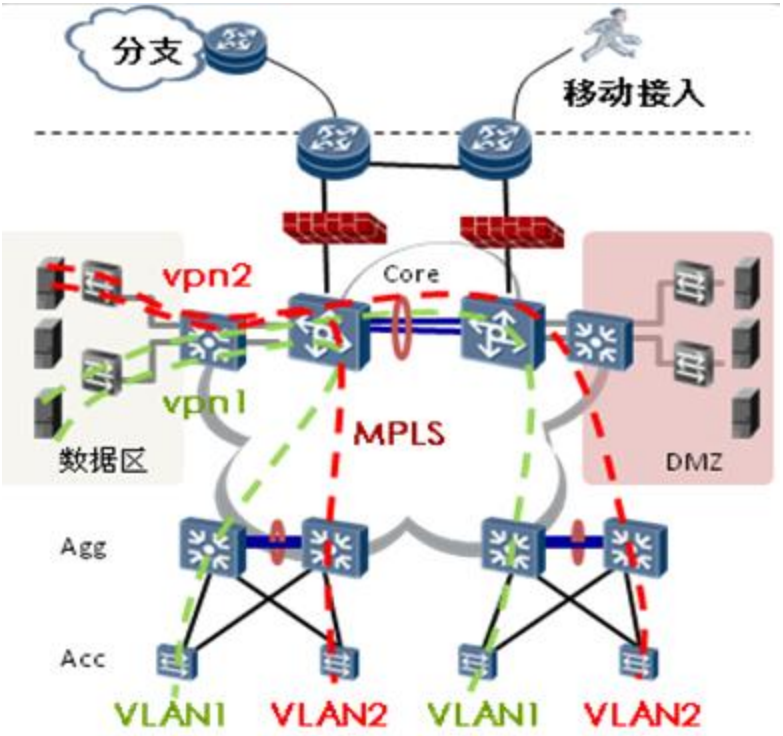
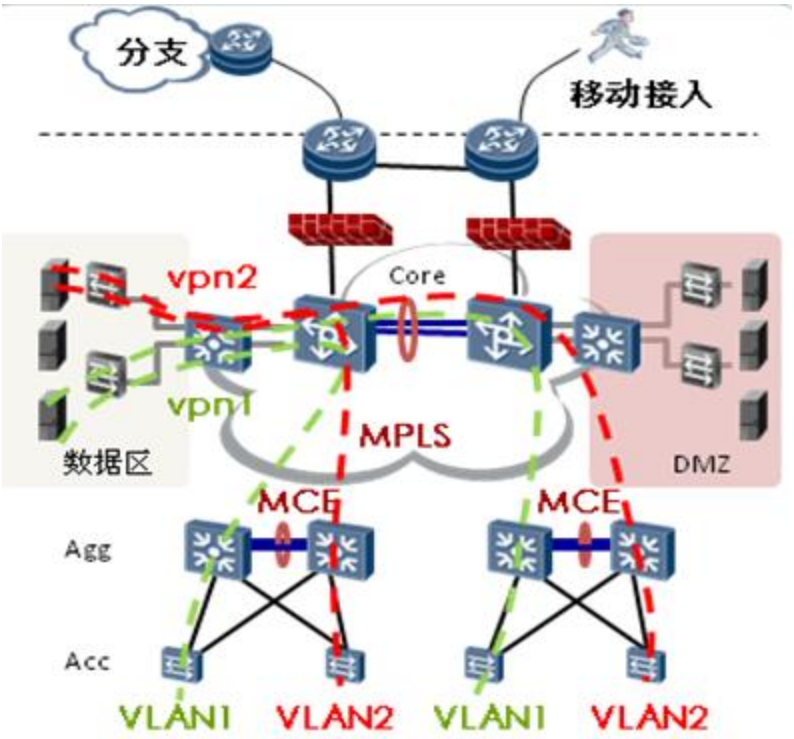


图4-7 核心层上部署 MPLS VPN



无论是汇聚层上部署 MPLS VPN，还是在汇聚层部署上 MCE 和核心层上部署 MPLS VPN，在接入层均需要通过 VLAN 隔离。PC 客户端上线发起认证，认证服务器根据认证结果下发 VLAN 到用户接口，使不同用户通过不同 VLAN 进入相应的 VPN。MCE/PE 设备会为每个 VPN 建立独立的路由转发表项，从而保证各 VPN 路由信息相互隔离不受影响，各 VPN 独立进行数据转发。

数据中心区中的服务器一般采用静态 IP 地址，不存在发起认证，下发 VLAN 的情况。所以要求服务器根据应用和访问用户的不同，也将端口加入到相应的 VPN 中。从 PC 用户到服务器，MPLS VPN 提供了端到端的业务传输通道，把不同用户组、不同应用的数据进行了安全隔离。

数据中心服务器根据应用情况可以分为：

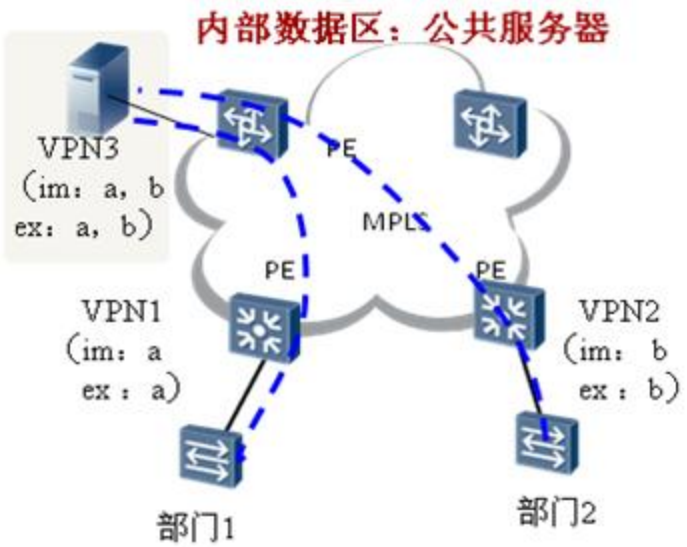
- 公共服务器：为不同部门或者不同安全级别用户组提供公共的应用服务。
- 独享服务器：专门为一个部门或者相同安全等级用户组提供独享的应用服务。
- DMZ 服务器：为 Internet 用户提供 WEB、Email 等 Internet 增值服务。

MPLS L3VPN 可以通过 RT 属性控制路由的发布、选择，从而实现灵活的组网方式，根据数据中心服务器三种不同应用可以分为三种场景。

- 公共服务器 VPN 部署方式

  如图 4-8 所示，在公共服务器 VPN 部署方式中，部门 1 和部门 2 均可以访问服务器资源，部门之间不能相互访问，可以采用 Extranet 组网方案。 VPN1、VPN2 需要访问 VPN3 共享站点，则 VPN1、VPN2 的 Export Target 必须包含在共享站点的 VPN3 实例的 Import Target 中，而其 Import Target 必须包含在共享站点 VPN3 实例的 Export Target 中。

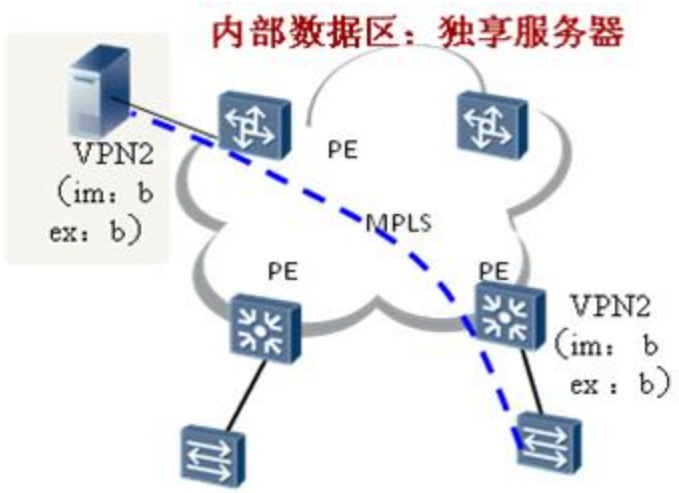
图4-8 公共服务器 VPN 部署方式



- 独享服务器 VPN 部署方式

  如图 4-9 所示，在独享服务器 VPN 部署方式中，是最基本的 MPLS VPN 模型，VPN 路由信息独立维护，不存在跟其他 VPN 的路由交互。

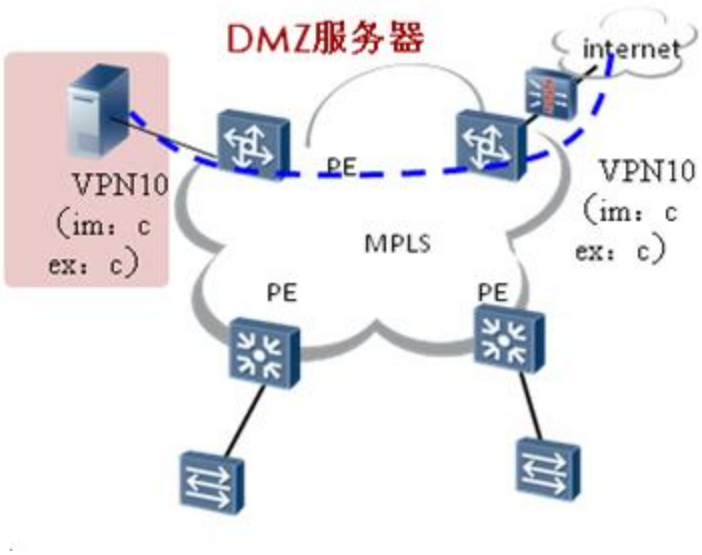
图4-9 独享服务器 VPN 部署方式



- DMZ 服务器 VPN 部署方式

  如图 4-10 所示，DMZ 服务器 VPN 部署方式跟独享服务器 VPN 部署方式类似，不同点在于服务器 IP 地址通过 VPN 传输通道到达防火墙后需要进行 NAT 公私网地址转换。

图4-10 DMZ 服务器 VPN 部署方式



采用 MPLS VPN+VLAN 或者 MPLS VPN+MCE+VLAN 方式隔离业务有如下特点：

- 资源利用率高、扩展性强，可以容纳 VPN 数量很大，同一 VPN 用户很容易扩充。特别适合大中型园区网络。
- 采用私有路由表实现业务隔离，不同的 VPN 处在不同的转发表项中，逻辑结构清晰，维护简便。

- MPLS VPN 支持灵活的访问控制策略，可以实现灵活的组网方式，如 Extranet 组网方式、Hub&Spoke 组网方式，更容易满足企业对业务多样性隔离部署的需求。

4.2 WLAN 解决方案

4.2.1 企业无线园区网的发展及设计需求

随着技术的发展和大量移动终端的出现，金融企业园区也从最初的有线覆盖网络形式历经有线无线覆盖网络到现在的无线泛在覆盖网络形式。

图4-11 企业园区网的无线化发展示意

由于无线网络覆盖场所的多样性、用户上网行为的复杂性、企业对于网络安全和网络质量的需求，需要在进行 WLAN 规划时除了 WLAN 组网以外，还需考虑到 WLAN 网络的通信质量、网络安全、可靠性、统一管理以及部分行业对无线用户接入认证、授权的需求。

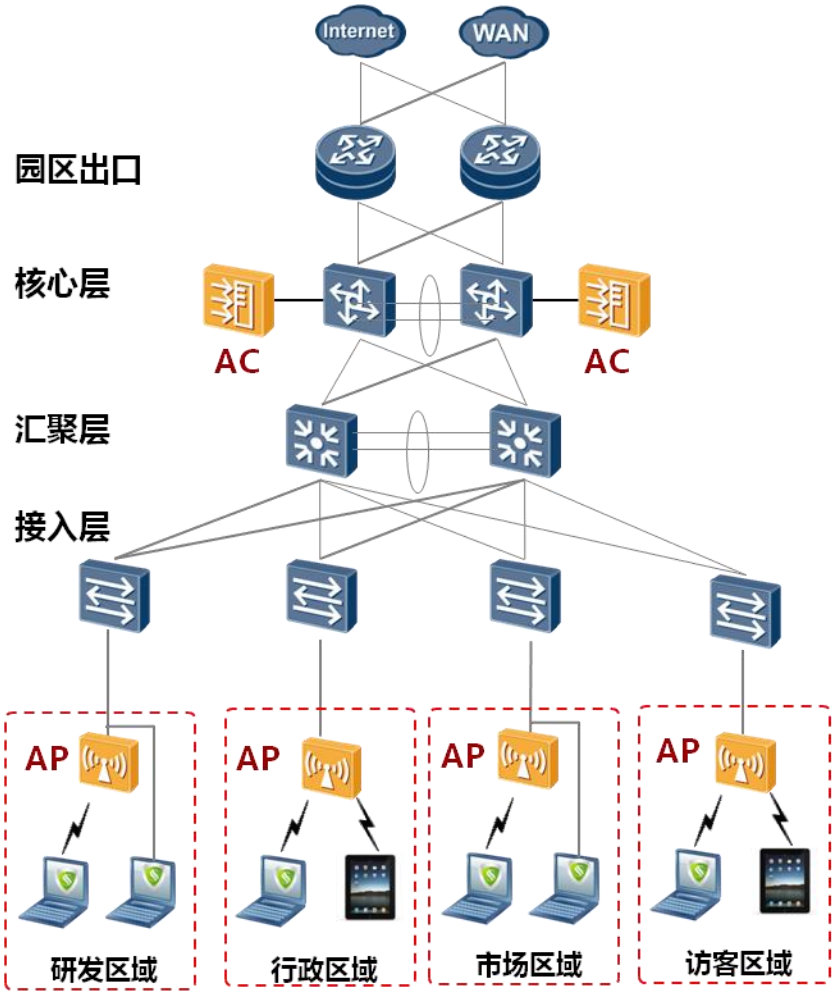
4.2.2 金融企业园区 WLAN 网络常用部署形式

WLAN 网络在部署过程中，根据不同的需求有多种实现形式，比如根据网络架构分可分为自治式架构（即 FAT AP 或胖 AP）和集中式架构（即 FIT AP 或瘦 AP）；在 FIT AP 网络架构下，又可以根据 AC 位置和部署形式的不同分为以下几种：

- 根据 AC 部署方式，分为集中式和分布式
- 根据 AC 部署位置，分为旁挂和直连
- 根据 AC 硬件体现形式，分为集成 AC 和独立 AC
- 根据业务转发形式，分为独立转发和集中转发

而在金融企业园区内，出于对集中管理、集中认证和集中安全管理的考虑一般采取集中式架构，根据园区规模选取独立 AC 旁挂于核心/汇聚交换机或交换机 ACU 插卡，实现对核心/汇聚交换机设备下所有 AP 的管理，如下图：

图4-12 金融企业园区 WLAN 网络



此架构下，AC 完成网络具有重要意义的功能，例如移动管理、身份验证、VLAN 划分、射频资源管理、无线 IDS 和数据包转发等；AP 完成无线空口的控制，例如无线信号发射与探测响应、数据加密解密、数据传输确认、空口数据优先级管理等功能。

AP 和 AC 间采用 CAPWAP 隧道协议进行通讯，AC 与 AP 间可以是直连、或者穿越 Layer 2、Layer 3 网络。

CAPWAP 协议是基于 UDP 传输层的应用层协议，协议传递的信息分为两类：控制信息和数据信息。

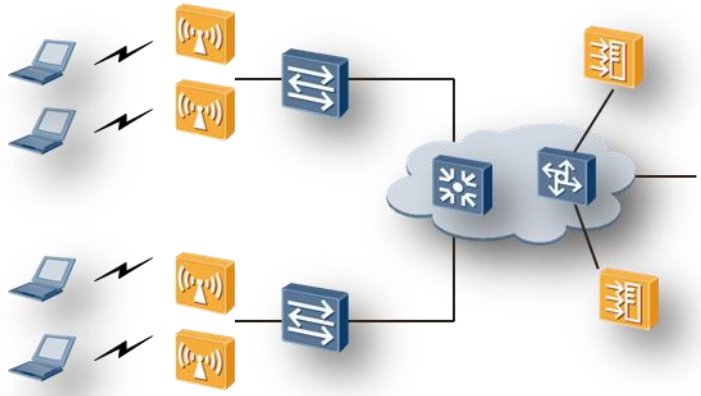
- 控制信息负责 AC 与 AP 之间的管理的交互操作，包括 AP 自动发现 AC、AC 对 AP 进行安全认证、AP 从 AC 获取软件版本、AP 从 AC 获取配置等等。
- 数据信息是封装后转发的无线数据。

两类信息分别使用不同的 UDP 端口号。CAPWAP 信息在 AP 与 AC 间交互时可以使用 DTLS 加密机制，保证通信的安全性。

根据园区规模选择 AC 的部署方式，中小型金融企业园区网络可进行集中式 AC 部署，大型园区可选取分布式 AC 部署。

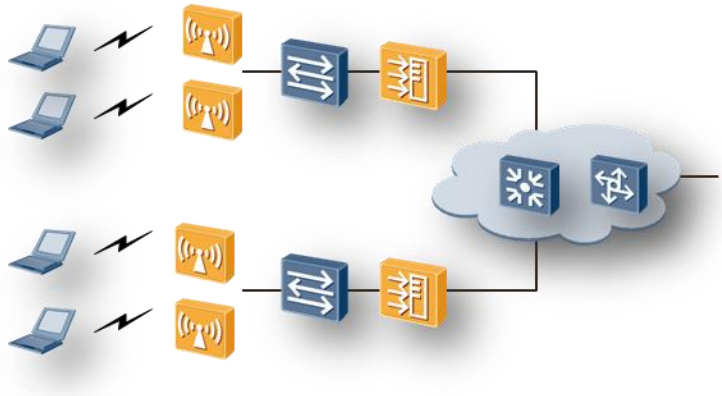
- 集中式 AC 部署：是指整个网络中集中部署 AC 设备（一般是独立的 AC 设备），来控制和管理整网的 AP 设备。AC 的部署可以采用直路（直接部署在 AP 和汇聚/核心交换机之间）或旁挂方式（旁挂在汇聚/核心交换机旁侧）。

图4-13 集中式 AC 部署示意图



- 分布式 AC 部署：是指网络中分区域采用多个 AC 设备，分别对本区域的 AP 设备进行管理。分布式 AC 方案一般不采用独立的 AC 设备，而是采用在汇聚交换机上集成 AC 功能，来实现对本交换机下挂的所有 AP 进行管理。

图4-14 分布式 AC 部署示意图



两种部署方式的优劣势对比如表 4-1 所示。

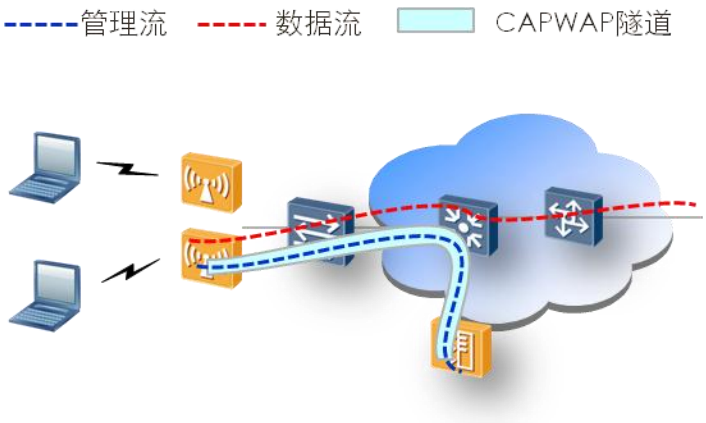
表4-1 集中式 AC 与分布式 AC 优缺点对比表

AC 方式	优点	不足
集中式	1、 节省投资 2、 容量管理更简单有效，成本效益高 3、 无线网络结合到已有的有线网络时，无线业务终结点少，便于管理 4、 漫游部署简单高效 5、 无线网络运维管理更简单，可集中管理且配置灵活	AC 与 AP 之间的网络结构复杂，网络规划部署相对复杂
分布式	AC 与 AP 之间网络结构简单，网络部署相对简单	1、 投资成本高 2、 需要部署 AC 间漫游；除非各 AC 所在的区域间不考虑漫游 3、 无线网络运维成本大

转发模式主要是 AP 针对用户数据可以有不同的转发处理方式。

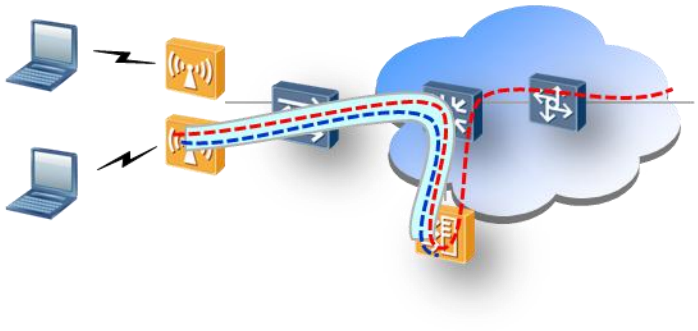
- 独立转发：又称直接转发，是指 AP 上对用户数据由本地转发到网络上层，不经过 AC 处理，AC 只对 AP 进行管理。而 AP 管理流封装在 CAPWAP 隧道中，到达 AC 终止。

图4-15 独立转发示意图



- 隧道转发：是指 AP 将用户数据、自身管理数据统一封装在 CAPWAP 隧道中，发送至 AC，由 AC 统一转发。

图4-16 隧道转发示意图



独立转发与隧道转发优缺点对比如所示。

表4-2 独立转发与隧道转发优缺点对比表

转发方式	优点	不足
独立转发	设备管理级部署简单，数据流量不经过 AC，AC 负担小	-
隧道转发	“业务管理级”部署流量全部经过 AC 可以按用户需求规划一些安全监管策略	AC 数据压力较大，对 AC 设备本身处理能力要求较高

对于金融企业园区，由于业务安全性要求较高，可以根据需要选取隧道转发方式进行数据转发。

4.2.3 WLAN 基础网络规划

IP 地址规划

1. AC 的 IP 地址

AC 用于管理 AP，IP 地址一般通过静态手工配置。

2. AP 的 IP 地址

AP 的 IP 地址分配如果采用静态分配，由于一般 AP 数量较多，配置工作量大，且容易冲突、不易于控制，所以不建议使用，建议使用 DHCP 动态分配。

DHCP 动态分配 AP 的 IP 地址时，可以有以下几种方式：

- 指定地址池分配
  - 根据 DHCP Option 60 表明 AP 身份而分配指定地址池的 IP：

    AP 的 DHCP Discover 报文携带 Option 60，例如内容为“Huawei AP”，表示请求分配 IP 地址的设备是华为 AP，而不是 WLAN 用户。DHCP Server 可以通过匹配或部分匹配 Option 60 字符串，来为 AP 从指定地址池中分配地址。

如果网络中部署多个 DHCP Server 且只有部分支持 Option 60，交换机等设备充当 DHCP Relay 时需要支持识别 DHCP option 60 并将 DHCP 报文转发到相应的 DHCP Server 上。

- 根据 VLAN 分配指定地址池的 IP：

  AP 相连交换机端口以 Trunk 方式加入 VLAN，允许通过的 VLAN 对应的地址池即为 AP 分配 IP 地址。

- 根据 AP 的 MAC 地址指定分配：

  在 DHCP Server 上配置 AP 的 MAC 以及对应的 IP 地址。

- 统一分配

  AP 的 IP 地址分配同 WLAN 用户一样，由 DHCP Server 统一分配，不再区别。

DHCP 动态分配 AP 的 IP 地址各种方式优劣势对比如表 4-3 所示。

表4-3 DHCP 动态分配 AP 的 IP 地址各种方式优劣势表

IP 地址分配方式		优势	劣势	适用场景
指定地址池分配	DHCP Option 60	AP 设备与无线用户的 IP 地址分离	需要交换机配套支持	对设备 IP 地址管理与用户 IP 地址管理要求隔离的
	根据 VLAN	AP 设备与无线用户的 IP 地址分离	网络配置工作量较大，不利于 AP 即插即用	对设备 IP 地址管理与用户 IP 地址管理要求隔离的
	根据 MAC	AP 设备与无线用户的 IP 地址分离	配置工作量较大，IP 地址管理难度加大	对少量 AP 设备管理有特殊要求的
统一分配		网络配置简单	-	对 AP IP 管理没有要求

3. 无线终端/用户的 IP 地址

   移动用户通过 DHCP 动态分配 IP 地址，不建议静态配置；对于基本不移动的无线终端（比如：无线打印机）可以静态配置。

SSID 规划

企业园区无线网络一般按照业务类型划分不同的 SSID（Service Set Identification）。

- SSID 映射以太网中的 VLAN

  通常，以太网中管理 VLAN 和业务 VLAN 分离。业务 VLAN 主要用于区分不同的业务类型或用户群体。

  在 WLAN 网络中 SSID 也同样可以承担相应的工作。因此，在业务 VLAN 的规划中必须综合考虑 VLAN 与 SSID 的映射关系。业务 VLAN 应根据实际业务需要与

SSID 匹配映射关系，映射关系有 1:1、1:N、N:1、N:N 四种，AC 设备终结 VLAN 部署。

- VAP 构建

  AP 可以配置多个 SSID，华为单频 AP 可支持 16 个 SSID，双频 AP 可支持 32 个 SSID。通过配置多个 SSID，可以将一个 AP 划分为多个 VAP（Virtual Access Point），每一个 SSID 对应一个 VAP，AC 针对 VAP 进行策略下发，VAP 根据策略进行终端与业务管理。

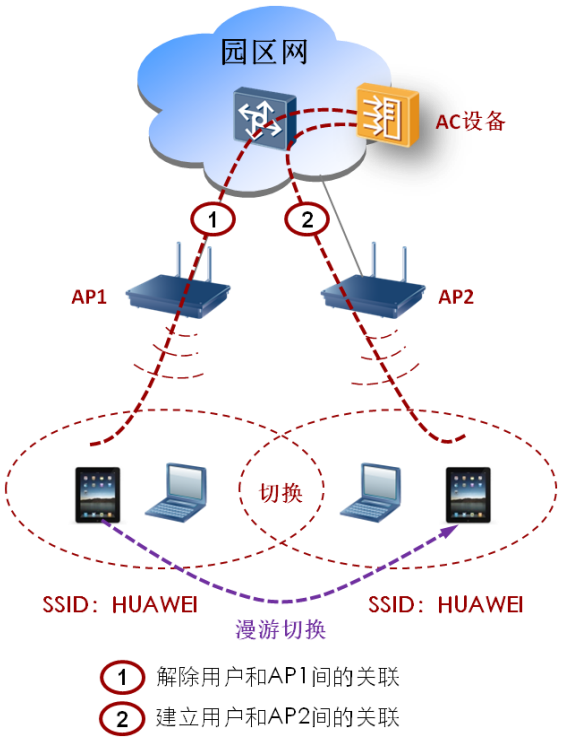
漫游规划

漫游是指用户在部署了 WLAN 网络的场所移动时，用户终端可以从一个 AP 的覆盖范围移动到另一个 AP 的覆盖范围，用户无需重新登录和认证。

如图 4-17 所示，假设终端与 AP1 已经建立关联信息，随着用户位置的移动，终端切换到 AP2，具体切换流程如下：

1. 客户端在各种信道中发送 802.11 请求帧。AP2 在信道 6（AP2 使用的信道）中收到请求后，通过在信道 6 中发送应答来进行响应。客户端收到应答后，对其进行评估，确定同哪个 AP 关联最合适。
2. 如图中的标号 1 所示，删除用户与 AP1 现有的关联。客户端通过信道 1（AP1 使用的信道）向 AP1 发送 802.11 解除关联信息，解除用户与 AP1 间的关联。
3. 如图中的标号 2 所示，客户端通过信道 6 向 AP2 发送关联请求，AP2 使用关联响应做出应答，建立用户与 AP2 间的关联。

图4-17 用户漫游切换示意图



WLAN 网络漫游中需注意以下两点：

- 漫游切换需要保证 SSID 相同，即两台 AP 切换区域需要配置相同的 SSID。
- 漫游切换 AP 必须是同一个 AC 管理。

AP 发现并选择 AC 方式规划

FIT AP 架构下的 WLAN 网络中，FIT AP 为零配置，当 FIT AP 部署到网络的时候，AP 需要去找到相应的 AC，并从 AC 上下载其配置。

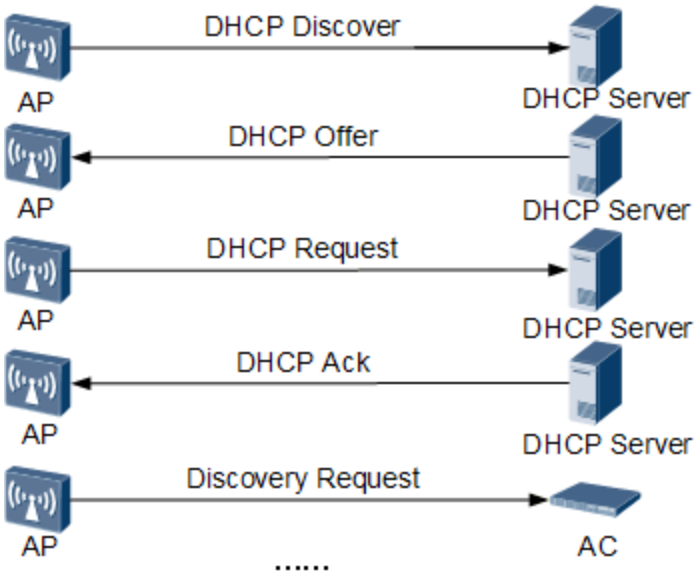
AP 发现 AC 的机制有如下几种：

- 二层广播发现 AC

  当 AC 和 AP 同在一个二层的网络中时，可以通过二层广播方式直接发现 AC。
- 通过 DHCP Option 43 发现 AC

  Option 43 是 DHCP 协议的一个属性，在华为 WLAN 网络里，AP 用它识别 AC 的 IP 地址。当 DHCP Server 配置了 Option 43 后，它给 AP 分配 IP 时，在 DHCP Offer 报文中同时会将此属性告知 AP。

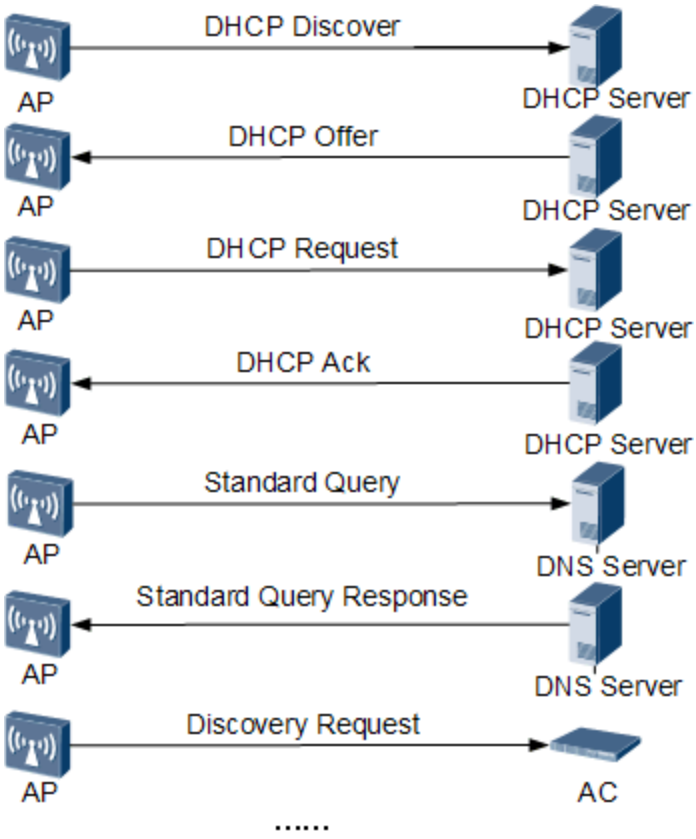
图4-18 通过 DHCP Option 43 发现 AC 的报文交互图



- 通过 DNS 发现 AC

  当网络中部署了 DNS Server 时，还可以通过 DNS 方式让 AP 来发现 AC。需要在 DHCP Server 上配置 DNS Server IP 地址以及 AC 的域名。当 AP 通过 DHCP 服务器获取 IP 地址时，DHCP Server 会在 DHCP Offer 报文中将 DNS 服务器 IP 地址（Option 6）和 AC 域名（Option 15）告知 AP，在 AP 获取到 IP 地址后，则通过 DNS 服务器解析到 AC 的 IP，从而实现对 AC 的发现和关联。

图4-19 通过 DNS 发现 AC 的报文交互图



- AP 上预配置 AC 列表

  AP 可以预配置 AC 的 IP 地址列表。当预配置好 AC 列表时，AP 将不再启动正常的 L2 或 L3 的发现过程，故 AC 列表里的地址不可达时，AP 将永远连接不上 AC。

上述几种方式优劣势对比如下表 4-4 所示。

表4-4 AP 发现并选择 AC 方式优劣势对比表

方式	部署要求	优势	劣势	适用网络
DHCP Option 43	DHCP Server 启动 Option 43 属性	适用于 AP/AC 任何组网中	对网络有部署要求	大中型 WLAN 网络，AP/AC 二层或三层组网
DNS	部署 DNS Server；DHCP Server 支持 Option 15 属性			
二层广播发现	无	对已有网络没有额外要求	仅能用于 AP/AC 二层组网中	小型 WLAN 网络，AP/AC 二层组网

方式	部署要求	优势	劣势	适用网络
AP 上预配置静态 AC 列表	AP 预配置	对已有网络没有额外要求	需要对 AP 逐一进行配置，工作量大；若 AC 的 IP 地址发生变化，则需要重新修改 AP 的配置	小型 WLAN 网络

若无线网络部署了多个无线控制器，AP 通过上述某种方式发现了多个 AC 时，AP 根据根据 AC 负载动态选择接入到负载轻的 AC。

射频管理规划

与 IP 地址规划一样，WLAN 信道是 WLAN 网络设计中的重要一环，大型无线园区网网络必须对 WLAN 信道进行统一规划。

WLAN 信道规划的好坏，影响到无线网络的带宽、无线网络的性能、无线网络的扩展以及无线网络的抗干扰能力，也必将直接影响到无线网络的用户体验。

1. 射频信道划分

WLAN 信道规划是 WLAN 网络设计中的重要一环，为保证信道之间不相互干扰，大型无线园区网网络必须对 WLAN 信道进行统一规划并实施。WLAN 系统主要应用于两个频段：2.4GHz 和 5.0GHz。

- 2.4GHz 频段信道划分：
  - 2.4G 频段具体频率范围为 2.4～2.4835GHz 的连续频谱，信道编号 1～14。
  - HT20 信道划分：信道带宽为 20M，在该模式下，一般选取 1、6、11 三个不重叠信道，频率规划可用频点只有 3 个。
  - HT40 信道划分：信道带宽为 40M，受频率限制，只支持一个不重叠信道。
- 5.0GHz 频段信道划分：
  - 5.0G 频段分配的频谱并不连续，主要有两段：5.15～5.35GHz、5.725GHz～5.85GHz。
  - HT20 信道划分：不重叠信道在 5.15～5.35GHz 频段有 8 个，分别为 36、40、44、48、52、56、60、64；在 5.725GHz～5.85GHz 频段有 4 个，分别为 149、153、157、161。
  - HT40 信道划分：在该模式下，这两段频谱的可用信道分别为 4 个和 2 个。

AP 支持手动和自动两种方式设置工作信道。设置为自动方式后，一旦检测到信道冲突 AP 具有信道自动调整功能，建议 AP 采用自动设置工作信道方式，避免手动设置后一旦信道冲突将导致无法切换信道的问题。

信道自动扫描功能：采用信道自动扫描功能，自动探测周边的 AP、使用的信道及干扰，结果上报 AC，触发信道调整。

2. 射频信道覆盖

WLAN 信道规划需遵循两个原则：蜂窝覆盖、信道间隔。根据覆盖密度、干扰情况、选择 2.4G/5G 单频或双频覆盖。AP 交替使用 2.4G 的 1、6、11 信道及 5.0G 的 36、40、44 信道，避免信号相互干扰；一般情况单独使用 2.4G 或 5.0G 的频段，对于会议室等高密度用户接入的场所，可以启用双频进行覆盖，以便提供更好的接入能力。

图4-20 单频信道规划示意图

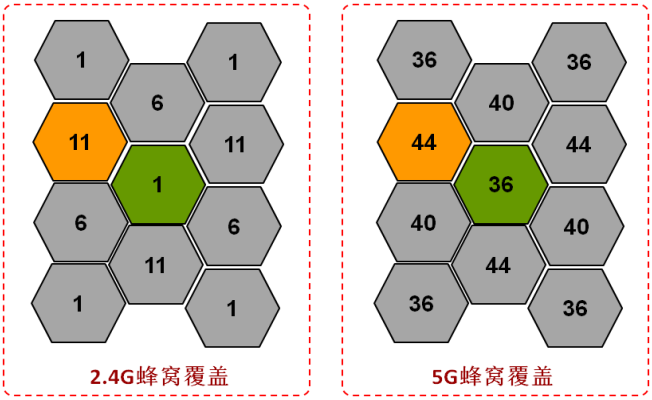
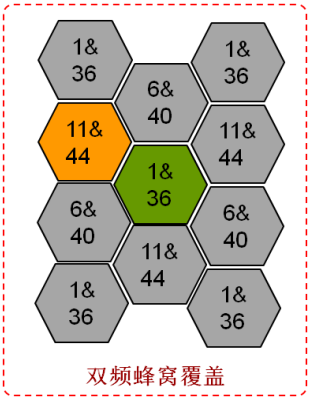


图4-21 双频信道规划示意图



无线网络安全规划

1. 无线设备安全

- AP 防盗

  安装 AP 时安装防盗锁即可。

- AP 零配置

  传统的 FAT AP 组网模式要求在 AP 上配置大量的业务参数，同时需要在 AP 本地保存这些业务配置信息，一旦设备丢失，AP 的业务配置信息就可能被泄漏，形成网络的安全漏洞。FIT AP 在设备上不保存业务配置，而是每次启动的时候从无线控制器动态加载业务配置，这样可以有效避免设备丢失造成配置泄漏。

  当前 FIT AP 均能做到零配置。

2. 无线 IDS/IPS

- IDS——非法 AP 检测

  非法 AP 主要指未经网络许可而非法部署的 AP 设备或者是对网络发起无线攻击的 AP 设备。

  对于非法部署的 AP 设备，可以通过控制 AP 接入（基于 MAC 地址；基于设备名称 SN 等）来防止非法 AP 接入网络。

  对于对网络发起无线攻击的 AP 设备，网络中合法部署的 AP 监听设备负责把监听到有攻击行为的无线设备上报给无线控制器，继而上报给网管。

  部署建议：

  - 对于非法部署的 AP 设备，由网络设备 AC 检测，启动相应功能即可。
  - 这里主要给出对发起无线攻击的 AP 的监听部署方案以及对比情况，如表 4-5 所示。可以根据实际网络要求进行取舍。

表4-5 对发起无线攻击的 AP 的监听部署方案优劣势对比表

部署方式	优点	劣势
部署专职监听 AP	实时监听网络，及时检测出非法 AP	网络部署成本高
业务 AP 兼职监听 AP	网络部署成本相对小	不能实时监听网络，无法及时检测到非法 AP

- IPS----黑白名单

  用户白名单功能：无线控制器支持静态配置白名单功能，该功能一旦启用，只有白名单上的无线用户才被认为是合法用户，其他非法用户的报文全部在 AC 上被丢弃，从而减少非法报文对无线网络的冲击。

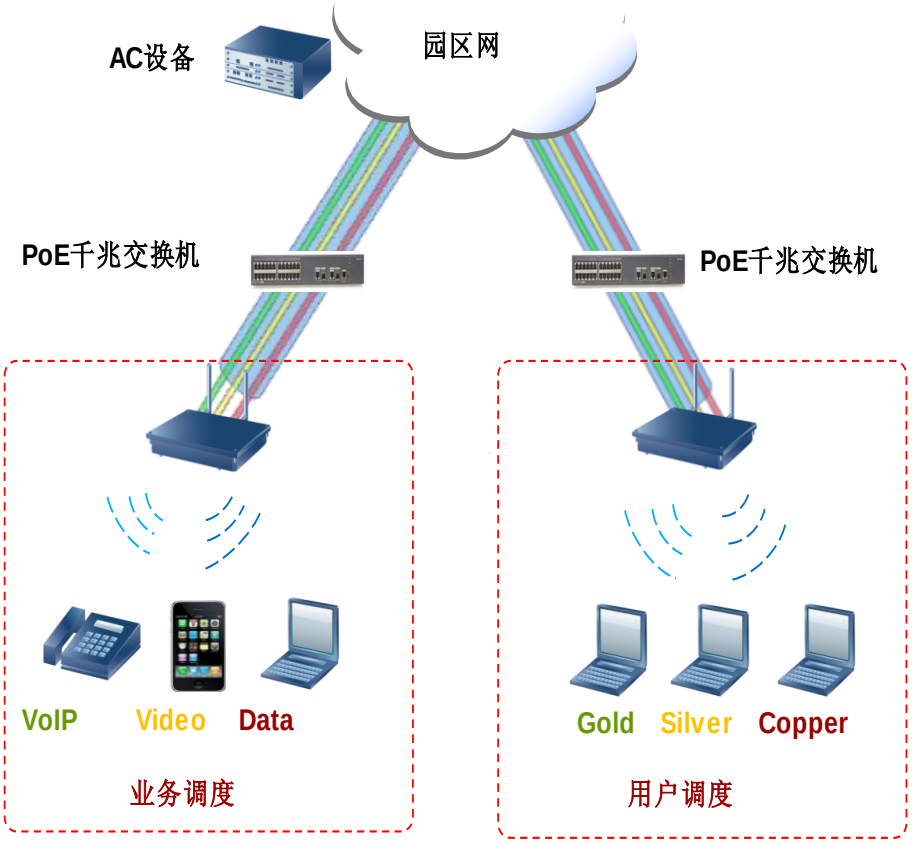
  用户黑名单功能：无线控制器通过配置方式或者实时检测侦听的方式来确定设备是否被加入黑名单，被加入到黑名单中的设备发过来的报文全部在 AC 上丢弃，从而减少攻击报文对无线网络的冲击。

  部署建议：大中型园区网不建议部署，通过认证进行用户的合法检测即可。

QoS 规划

WLAN QoS 保证不同质量的无线接入服务之间的互通，满足实际应用的需求。

图4-22 WLAN QoS 规划



如图 4-22 所示，在企业园区中，常采用无线空口做 WMM 调度，有线侧进行优先级映射，园区网做 DiffServ 调度的方式，最大程度优化网络发生拥塞时的核心业务和 VIP 用户服务质量。在这里仅介绍 WMM 协议技术、优先级映射和流量管理技术。

- 流量管理
  - 基于用户的流量管理

    防止 P2P 业务占用带宽导致其他用户无法正常使用无线网络，比如校园网。
  - 基于 SSID 的流量管理

    防止某些 SSID 用户流量过大影响其他 SSID 用户的正常业务，比如访客 SSID 的流量控制。
- 无线空口做 WMM 调度

  Wi-Fi 多媒体标准 WMM（Wi-Fi Multimedia）是一种无线 QoS 协议，无线空口上，WMM 将数据报文通过 4 个优先级队列发送，每个优先级队列占用信道的机会不一样，从而保证语音、视频等应用在无线网络中有更好的质量。

  WMM 按照优先级从高到低的顺序分为 AC（Access Category）-VO（语音流）、AC-VI（视频流）、AC-BE（尽力而为流）、AC-BK（背景流）四个优先级队列，保证越高优先级队列中的报文，抢占信道的能力越高。

表4-6 WMM 队列优先级

WMM 队列	用户优先级（UP）
Voice	6 或 7
Video	4 或 5
Best Effort	2 或 3
Background	0 或 1

- 优先级的映射

  优先级映射包括：无线优先级到有线优先级的映射、无线优先级到 CAPWAP 隧道优先级的映射。

  - 上行无线到有线报文优先级映射

    AP 接收到无线客户端发送的 802.11（无线）数据报文后，将其转换为 802.3（以太网）报文，然后向网络侧继续转发。对于本地转发，完成用户优先级 UP 到 802.1P 优先级映射；对于集中转发，再实现隧道优先级 Tunnel-802.1P、Tunnle-TOS 的映射。

  - 下行有线报文到无线报文优先级映射

    AP 接收到 802.3 以太报文后，将其转换为 802.11 报文，并在空口上依据报文中的 UP 优先级选择不同的 WMM 队列发送给用户终端。对于本地转发，需要完成 802.1P 到 UP 优先级映射；对于集中转发，在 AC 上可实现 TOS 优先级到 Tunnel-TOS 映射，802.1P 优先级到 Tunnle-802.1P 优先级映射。

可靠性规划

WLAN 网络可靠性主要是网络的负载分担，分为 AP 负载分担和 AC 的负载分担。

- AP 负载分担

  无线客户端一般会根据 AP 信号强度（RSSI）选择 AP，这很容易导致大量的客户端仅仅因为某个 AP 信号较强而连接到同一个 AP 上。由于这些客户端共享无线媒介，导致每个客户端的网络吞吐将大量减少。AP 负载分担可动态地确定在当前时刻和当前位置下哪些 AP 可以彼此分担负载，通过控制无线客户端接入的 AP，来实现这些 AP 间的负载分担。

  评估负载的方式有两种：

  - 按照用户在线会话数
  - 按照用户流量

  当前 AP 负载分担策略是通过控制 STA 的接入实现负载均衡。当 AP 的负载情况超过阈值后，该 AP 就会拒绝新的终端的接入，此时终端将寻找负载较轻的 AP 进行连接，从而实现负载的均衡。

- AC 负载分担

  AC 负载分担即 AP 根据 AC 负载动态选择接入到负载轻的 AC 上去。

AC 在响应报文（Discovery Response）中携带该 AC 负载信息（比如 AC 允许接入的最大 AP 数、当前接入的 AP 数、允许接入的最大 STA 数、当前接入的 STA 数），AP 通过比较各 AC 的负载情况选择一个负载轻的 AC 接入。

通过 CAPWAP 隧道的心跳机制，AP 可及时发现控制器 Down，同时根据该方法重新选择一个负载轻的 AC 接入。

4.2.4 WLAN 接入认证方案

WLAN 终端认证技术

IEEE 802.11 标准要求 WLAN 终端在准备连接到网络时，必须进行“身份验证”。

WLAN 终端身份认证主要有两种方式：开放系统认证（Open-system Authentication）和共享密钥认证（Shared-Key Authentication）。

- 开放系统认证是 IEEE 802.11 标准要求必备的一种方法，是最简单的认证算法，即不认证。如果认证类型设置为开放系统认证，则所有请求认证的客户端都会通过认证。在这种方式下，接入点并未验证工作站的真实身份，工作站以 MAC 地址作为身份证明，这种验证方式可以让所有符合 802.11 标准的终端都可以接入到 WLAN 网络中来。开放系统身份验证比较适合有众多用户的电信运营 WLAN 网络。
- 共享密钥式认证必需使用加密方式，要求每个 WLAN 终端都配置和 AP 完全一致的密钥（key）。由于配置工作量较大，一般适用于企业网、校园网及家庭网络等。

二者对比如下：

表4-7 WLAN 终端认证方式对比

认证方式	优点	缺点	适用场景
开放式系统认证	部署简单，终端接入速度快，有效带宽高。	安全性差，无法检验客户端是否合法，任何知道无线局域网 SSID 的用户都可以访问网络。	电信运营网络
共享密钥式认证	安全性较高，采用加密方式对密钥进行保护，空口密钥数据不再明文传输。	配置复杂，可扩展性不佳；每台终端和 AP 上都需要静态配置一个很长的密钥字符串。 有效带宽较低，加密降低了传输效率。	企业网、校园网及家庭网络等。

无线用户身份认证技术

相对于简单的 STA 身份验证过滤机制，链路层用户身份验证的安全性大大提高。通过提供有限的访问权限来验证用户身份，只有确定用户身份后才给予完整的网络访问权限，可有效判别用户的合法性。链路层身份验证是透明的，能配合任何网络层协议使用。

常用的 WLAN 的链路层身份验证主要有 MAC 认证、802.1x、Portal（DHCP+Web）、PPPoE 等几种认证方式。

对于企业园区，无线哑终端一般通过 MAC 认证接入，办公区域通过 802.1x 或 Portal 认证接入，访客区域一般通过 Portal 认证接入。

多种认证技术保证 WiFi 终端安全接入，合法用户访问合规资源，从源头上消除安全威胁。

- MAC 认证

  MAC 认证是一种基于端口和 MAC 地址对用户的网络访问权限进行控制的认证方法，它不需要用户安装任何的客户端。由于无线终端的网卡都具备唯一的 MAC 地址，因此可以通过检查无线终端数据包的源 MAC 地址来识别无线终端的合法性。地址过滤控制方式要求预先在 AP 服务器中写入合法的 MAC 地址列表，只有当客户机的 MAC 地址和合法 MAC 地址表中的地址匹配，AP 才允许客户机与之通信。

  在企业园区中 MAC 认证主要用于 IP 电话、打印机等哑终端设备的接入。

- 802.1x 认证

  802.1x 是针对以太网而提出的基于端口进行网络访问控制的安全性标准草案。基于端口的网络访问控制利用物理层特性对连接到 LAN 端口的设备进行身份认证。如果认证失败，则禁止该设备访问 LAN 资源。

  尽管 802.1x 标准最初是为有线以太网设计制定的，但它也适用于符合 802.11 标准的无线局域网，且被视为是 WLAN 的一种增强性网络安全解决方案。802.1x 体系结构包括三个主要的组件：

  - 请求方（Supplicant）：提出认证申请的用户接入设备，在无线网络中，通常指待接入网络的无线客户机 STA。
  - 认证方（Authenticator）：允许客户机进行网络访问的实体，在无线网络中，通常指访问接入点 AP 或控制器 AC 设备。
  - 认证服务器（Authentication Sever）：为认证方提供认证服务的实体。认证服务器对请求方进行验证，然后告知认证方该请求者是否为授权用户。认证服务器可以是某个单独的服务器实体，也可以不是，后一种情况通常是将认证功能集成在认证方 Authenticator 中。

  802.1x 技术是一种增强型的网络安全解决方案。在采用 802.1x 的无线 LAN 中，无线用户端安装 802.1x 客户端软件作为请求方，无线设备 AP/AC 内嵌 802.1x 认证代理作为认证方，同时它还作为 Radius 认证服务器的客户端，负责用户与 Radius 服务器之间认证信息的转发。

  802.1x 体系本身不是一个完整的认证机制，而是一个通用架构。用来传输实际的认证协议。802.1x 体系的好处就是当一个新的认证协议发展出来的时候，基础的 802.1x 体系机制不需要随着改变。802.1x 体系使用 EAP（Extensible Authentication Protocol）认证协议，目前有超过 20 种不同的 EAP 协议。802.1x 认证常用的包括以下几种 EAP 认证模式：

  - EAP-MD5
  - EAP-TLS(Transport Layer Security)
  - EAP-TTLS(Tunnelled Transport Layer Security)
  - EAP-PEAP(Protected EAP)
  - EAP-LEAP(Lightweight EAP)
  - EAP-SIM

- PPPoE 认证

PPPoE 是 PPP 协议应用到以太网进行的再一次封装，进行广播链路上点对点通讯的协商，包括服务器的发现和会话标识 Session ID 的确认。主要包括三个部分：

- 用户和接入设备在 LCP 阶段协商链路层参数。
- 将用户名和密码发送给接入设备进行 CHAP/PAP 认证，接入设备可以进行本地认证，也可以将用户名和密码发送给 AAA 服务器进行认证。
- 根据认证结果，是否进入到 NCP（IPCP）协商阶段，接入设备给用户计算机分配网络层参数（例如 IP 地址等）。PPP 的三个协商阶段通过后，用户就可以发送和接收数据报文。

PPPoE 也是一种认证模式，PPPoE 在 WLAN 使用时，和 WLAN 本身采用的认证加密没有关系。即不管采用 WEP、WPA 或者 WAPI，都可以选择 PPPoE 作为用户业务的认证协议。

- Portal 认证

  Portal 认证也称 Web 认证或 DHCP+Web 认证。客户端使用标准 Web 浏览器（例如 IE），填入用户名、密码信息，页面提交后，由 Web 服务器和设备配合完成用户的认证。

  接入设备将来自客户的 HTTP 请求重定向到 Portal 服务器，在 Portal 页面上输入用户名、密码进行认证。用户在 Web 认证之前，必须先通过 DHCP、静态配置等获得 IP 地址。用户如果被配置成强制 Web 认证，则用户只需要输入自己喜欢的网页即可，系统自动下载认证网页。主要认证过程为：

  - 动态用户通过 DHCP 协议获取地址；
  - 用户访问 Web 认证服务器的认证页面，并在其中输入用户名、密码，Web 认证服务器将用户的信息通过内部协议，通知接入设备；
  - 接入服务器到相应的 AAA 服务器对该用户进行认证，将认证结果通知 Web 认证服务器；
  - Web 认证服务器通过 HTTP 页面将认证结果通知用户，如果认证成功用户即可正常访问网络资源。

  Portal 认证通常需要多个服务器支持，DHCP 服务器、AAA 服务器等。

无线接入认证和安全协议对应关系

表4-8 无线接入认证和安全协议对应关系表

认证方法	安全协议	安全性	封装开销	地址分配	客户端软件	应用场景
MAC 认证	Open System	低	小	认证后分配	不需要	PDA、IP 电话等哑终端设备接入。
	WEP/WPA/WPA2+PSK	低	小	认证后分配	不需要	场景同上，需要维护 PSK 密码。
Portal 认证	Open System	中	小	认证前分配	不需要	中小型园区网络。

认证方法	安全协议	安全性	封装开销	地址分配	客户端软件	应用场景
	WEP/WPA/WPA2+PSK	中	小	认证前分配	不需要	场景同上，需要维护 PSK 密码。
802.1x 认证	WEP/WPA/WPA2	高	小	认证后分配	需要	大中型园区网络。
PPPoE 认证	Open System	低	大	认证后分配	需要	运营商市场
	WEP/WPA/WPA2+PSK	低	大	认证后分配	需要	场景同上，需要维护 PSK 密码。

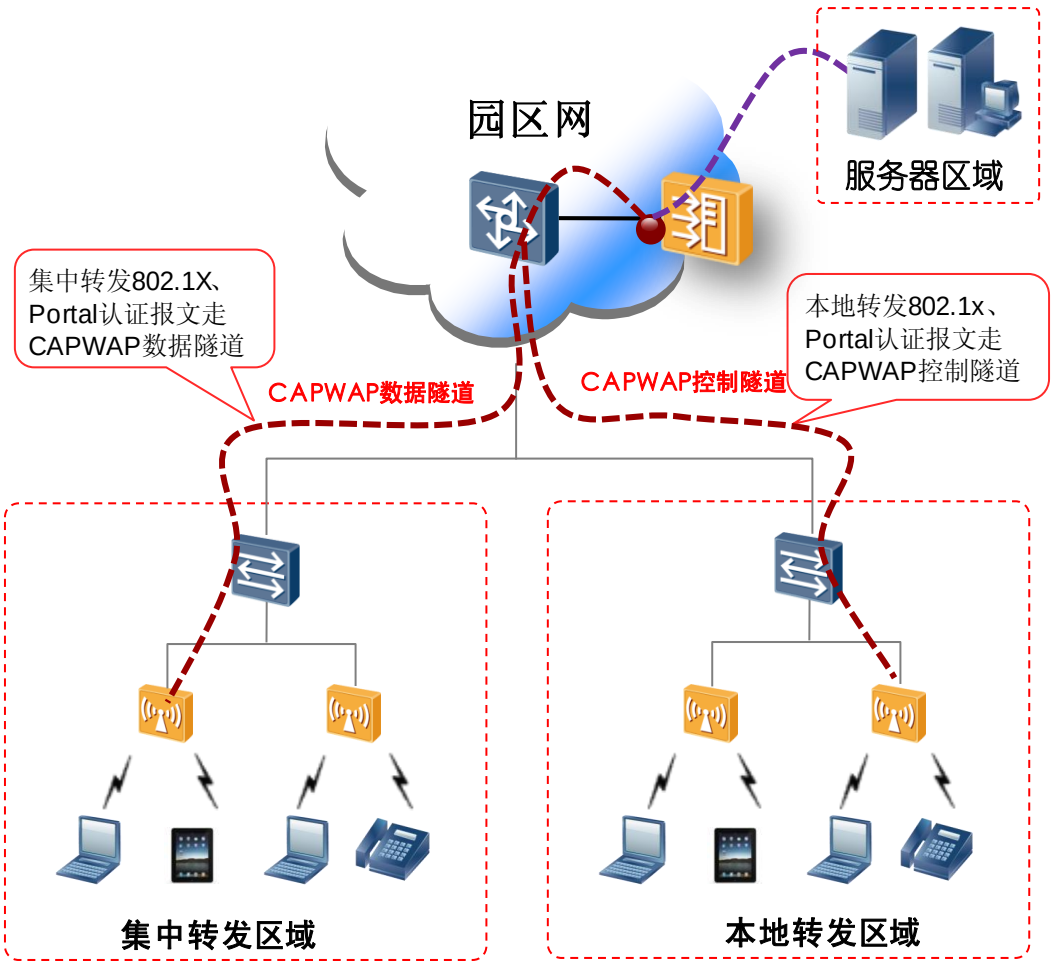
当前 WAPI 在企业网和运营商中应用很少，一般作为准入门槛测试，园区网中，从安全性和易部署性等多方面考虑，推荐 802.1x＋WPA2 的机制。

无线用户 AC 集中认证方案

无线用户在 AC 上集中认证，可以保证无线用户集中管理，授权通过 AC 控制隧道下发到 AP 设备，精细化控制用户访问权限，并在用户漫游、安全控制等方面由 AC 做到灵活控制。

无线用户集中认证，需要保证相关认证协议能够上送 AC 处理。集中转发场景下，EAP、Portal 报文作为数据报文通过 CAPWAP 数据隧道上送 AC；在本地转发场景下，可通过配置让 EAP、Portal 报文进入 CAPWAP 控制隧道，从而上送到 AC 设备完成认证过程。

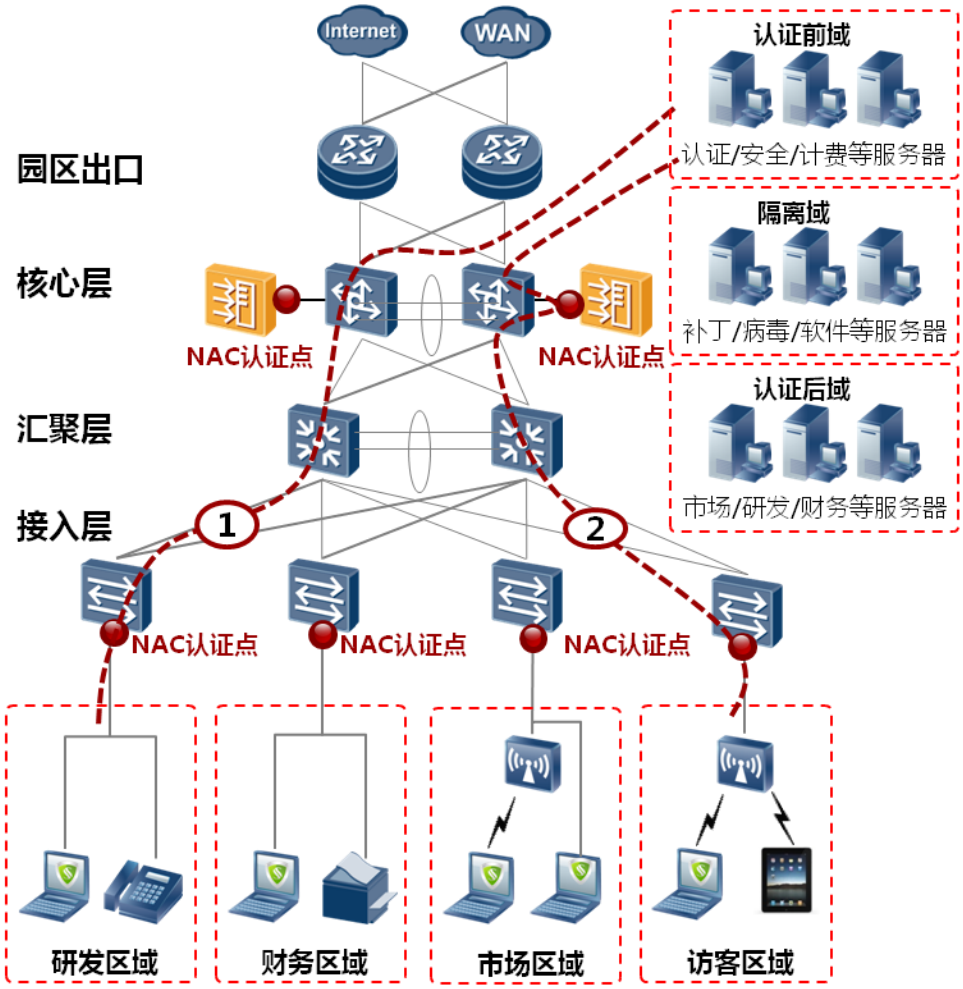
图4-23 无线用户 AC 集中认证示意图



AC 集中认证组网如图 4-23 所示，认证方式包括 MAC、802.1x、Portal、PPPoE 等方式。园区网中，从安全性、易部署等角度考虑，一般推荐 802.1x+WPA2 接入认证。

园区有线无线一体化认证方案

有线无线混合组网的接入模式是目前金融企业园区内的常用模式，华为有线无线一体化认证方案组网如下图所示：



本方案适合本方案适于大、中、小型园区，特别是用户对于安全控制要求严格的场景，可选择在接入层部署 802.1X＋MAC 混合认证方式。

其中，接入层交换机启用 802.1X＋MAC 自适应混合认证，有线用户做 802.1X 认证，IP 电话、打印机等哑终端做 MAC 认证。对于无线用户，在 AC 设备启用 802.1X 认证，无线终端通过 802.1X 认证接入园区。服务器系统为华赛 TSM 服务器组件，基于用户组进行用户管理和权限控制。接入层交换机要求为全部支持 802.1X＋MAC 认证设备。

此种方案控制点离用户最近，内网得到最大安全保障；同时由于采用 802.1X＋MAC 自适应混合认证，用户无需关注接入终端类型，方便网络部署。

4.3 语音解决方案

4.3.1 现网概况

企业不断面临着提高业绩、保持竞争力、实现盈利和迅速成长的挑战。在当前严峻的市场竞争中，一套强大的通信系统能为企业带来效率的提高，为企业的高速成长提供强有力的保障。

然而，传统的通信系统已不能满足当前丰富的通信需求，企业语音网络面临的通信需求主要集中在下面几方面：

- 企业内部的语音通信,可以通过企业自建的 IP 网络进行语音通信,而不需要从运营商的 PSTN 网络进行语音通信,使企业内部的语音通信不再需要通信费用,从而节省了企业的运营成本；
- IP 语音通信系统相对于传统的语音通信系统,可以很好的支持各种增值业务,从而丰富企业的通信手段，如:一号通业务,可以通过号码绑定,使客户不会错过任何一个商务电话；
- 传统的语音网络只能提供固定的电话服务,当前企业规模的扩大与人员办公流动性,传统的语音网络无法提供 UC 统一通信,无法做到无论何时,无论何地,无论何种接入都可以参与到企业的内部通信中；
- 可以通过 IP 网络,将企业传统的通信方法由 PSTN 网络切换到 IP 网络,从而使企业的 IP 网络与 PSTN 网络运行在同一张网上,有效降低了企业的运维成本。

随着“ALL OVER IP”愈演愈烈，业务统一承载已经是大势所趋。语音业务，也随着 VOIP 技术的成熟而快速向 IP 语音演化。

4.3.2 园区 IP 语音系统建设目标

企业为了充分利用内部建设的 IP 网络，节约电话通讯成本、开发新的应用、提高通信效率，同时企业的 IP 语音系统建设需要满足企业内部各分支之间的语音通信需求，同时还要为将来的用户数量的扩容及功能应用留下良好的扩展空间。

企业建设 IP 语音通信系统主要需要达到如下目标：

- 利用企业的 IP 网络,构建一个语音质量可以与 PSTN 网络相媲美；同时,将企业内的电话、传真、电话会议、即时消息、短消息等各种通信方式整合在一起，丰富员工的沟通手段，提高员工的沟通效率；
- 在企业系统内部建设一套完善的 IP 通信系统,同以满足企业内部各分支之间的 IP 语音通信能力；同时利用企业出口路由器设备与 PSTN/PLMN 网络进行互通；
- 利用企业的 IP 网络,构建的语音通信网络,可以很好的与公司的 IT 系统进行集成与整合,提升整体的工作效率；
- 利用企业的 IP 网络丰富的可靠性保护机制,可以有效的提高 IP 语音通信的业务和网络的可靠性。

4.3.3 园区语音系统设计原则

建设 IP 语音通信系统面临的挑战是如何在 IP 网络基础上,既可以保护原有投资和用户使用习惯,又可以让企业的语音业务和数据业务在同一张 IP 网络上协调运作,同时可以满足 IP 语音通信后续的发展及用户数量的扩容需求，华为的 IP 语音通信系统遵循以下的设计原则用来满足上述需求:

- 设备利旧原则

  利用企业的 IP 网络承载企业的语音通信业务，最大程度发挥 IP 网络的承载能力；对于企业原来通过 E1 接口入到运营商 PSTN 网络的 TDM PBX 设备，通过 E1 接口接到企业的 AR 设备上，达到充分利用 TDM PBX 设备。
- 企业语音部署结构选择原则
  - 企业分支集中在同一个号码区域时，建议采用集中式呼叫控制组网。

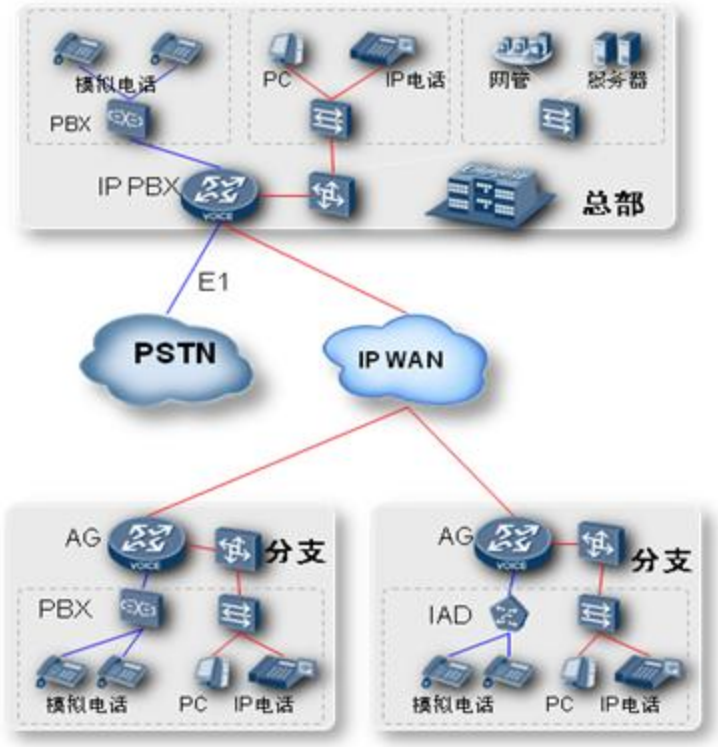
- 企业分支没有集中在同一个号码区域时，同时分支数量很多的情况下，建议采用多分支多级路由呼叫控制组网。
- 企业分支没有集中在同一个号码区域时，同时分支数量不多的情况下，建议采用多分支 Full Mesh 呼叫控制组网。

- 企业语音用户拨打外线出局选择原则
  - 企业是外贸型企业，企业的通信主要是对外通信，则建议企业向运营商申请的出局收敛比为 1：2 或者 1:1.5 。
  - 企业是生产型/研发型企业,企业的通信主要是内部通信，则建议企业向运营商申请的出局收敛比为 1:4~1:10 。

4.3.4 园区基础语音部署规划

集中式呼叫控制方案

图4-24 集中式呼叫控制方案图

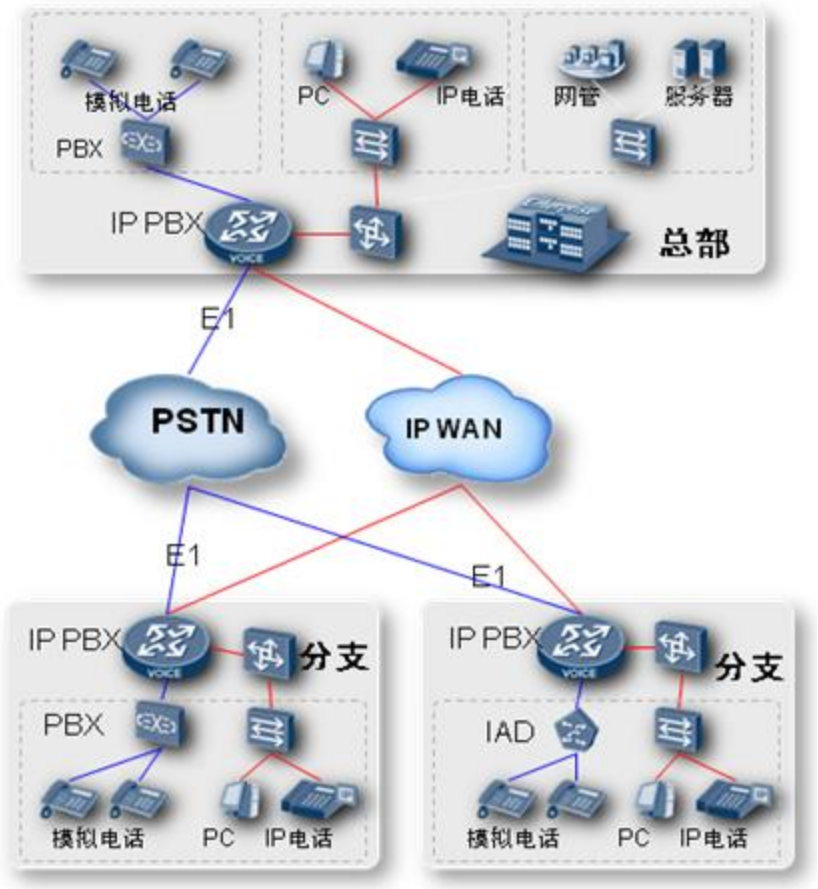


集中式呼叫控制模式，总部部署 IP PBX，各分支的 AR 部署为 AG，各分支和总部的用户注册到总部 IP PBX 上，总部 IP PBX 为园区内所有用户提供呼叫控制服务，AR 内置 SRST 功能。

总部 IP PBX 设备接入 PSTN 网络，实现总部及分支所有用户与 PSTN 用户的互通。

分布式呼叫控制方案

图4-25 分布式呼叫控制方案图



采用分布式多分支控制部署，总部以及各个分支的 AR 分别部署 IP PBX 功能。

各分支和总部的语音用户在本地完成用户注册和呼叫控制，总部 IP PBX 为各个分支互通提供呼叫路由，形成总部为一级呼叫路由，分支为二级呼叫路由的结构。

IP PBX 设备下挂 IAD 设备，一方面扩大了接入用户数量，另外一方面提供了 POST 话机的接入方式，实现模拟信号到数字信号的转换。

企业可以为分散在不同城市的办公分支提供 VOIP 服务，不同分支间可使用企业短号进行通话以及企业对分支所在地的外线呼叫，可通过 IP 网络承载，节省企业的通讯长途话费用。

本身具有 TDM PBX 的分支机构，AR 通过 E1 板卡将 TDP PBX 接入，保留客户原有投资。通过 LAN 扩展 IP phone 接入。所以分支机构（含总部）都通过 E1/FXO 接口接入到本地 PSTN 网络，并作为分支长途互通的备份。

总部部署 AR 3260 路由器及 Sx700 等型号交换机，提供约 1000 用户接入，根据分支规模，园区分支语音部署方式可以有如下几种选择：

- 对于<8 人的 SME 小型分支，部署 AR200 作为 IP PBX，满足基本语音业务，通过 FXO 口接入 PSTN 网络。
- 对于<32 人的小型分支，部署 AR1220 作为 IP PBX，通过模拟语音板卡，接入模拟话机，通过 LAN 口接入 IP 电话以及软终端，满足园区内基本语音业务，通过 FXO 口接入 PSTN 网络。
- 对于<200 人的中小型分支，部署 AR2220 作为 IP PBX，通过模拟语音板卡，接入模拟话机，可以接入 IAD 扩容模拟话机，通过 LAN 口接入 IP 电话以及软终端，满足园区内基本语音业务，通过 E1 中继接入到 PSTN 网络。
- 对于<500 人的中型分支，部署 AR2240 作为 IP PBX，通过模拟语音板卡，接入模拟话机，通过 LAN 口接入 IP 电话以及软终端，通过 E1 接入传统 TDM-PBX，满足园区内基本语音业务，通过 E1 中继接入到 PSTN 网络。

用户接入方式

- 模拟电话接入

  对于企业总部与分支，根据不同模拟用户的数量来选择不同的设备及组网方案，选择的标准主要是以企业内 POTS 语音用户的数量来衡量，相关的选择标准请参考如表 4-9 所示。

表4-9 用户通过模拟电话接入时园区网设备选择

序号	POTS 语音用户数	建议选择部件	后续扩容选择部件
1	8 人以下	1、AR200 2、AR 1200，配置 2 块 SIC 卡(支持 8 路 POTS 语音用户接入)	通过增加 IAD 进行扩容
2	32 人以下	AR 1200+IAD 132E(T)。IAD 132E(T)支持 32 路 POTS 用户，但是可以通过级联扩容到 96 路 POTS 语音用户接入	AR 2200，配置 1 块 WSIC 卡(最大支持 32 路 POTS 语音用户接入)
3	64 人以下	AR2200+IAD 1280。AR2200 最高可以支持 256 路语音用户接入，IAD 1280 最高可以支持 128 路 POTS 语音用户接入；	AR 2200，配置 2 块 WSIC 卡(最大支持 64 路 POTS 语音用户接入)
4	128 人以下	AR3200+IAD 1280。AR3200 最高可以支持 512 路 POTS 语音用户接入；	AR 3260，配置 4 块 WSIC 卡(最大支持 128 路 POTS 语音用户接入)

- IP 电话接入

  相对于模拟语音用户的接入，IP 语音用户具有安装快速、操作简单、统一布线等特点。

- 企业的 IP 网络布线到哪 IP 电话就可以直接通过企业的 IP 网络进行接入，可以通过企业的统一 DHCP Server 进行 IP 电话的地址分配。
- IP 电话自身具备对信令流及媒体流的 QoS 设置，从而保证了 IP 电话在企业 IP 网络中语音流量的优先处理，提高了 IP 电话在 IP 网络中的服务质量。
- IP 电话的网线如果是接在可以提供 PoE 供电的网络设备上，则 IP 电话的供电可以由网络设备通过 PoE 进行供电；如果 IP 电话接在不可以提供 PoE 供电的网络设备上，则 IP 电话的供电由 IP 电话的电源适配器进行供电。
- IP 电话的双网口设计。IP 话机提供两个 RJ-45 网口，可以分别连接网络设备和用户计算机，节省了企业的布线成本，提高了企业 IP 电话的快速安装。

企业出口多业务路由器 AR 根据不同的型号，可以支持的 IP 语音用户数也不同，具体规格如表 4-10 所示。

对于企业总部与分支，根据不同 SIP 语音用户的数量来选择不同的设备及组网方案，选择的标准主要是以企业内 SIP 语音用户的数量来衡量，相关的选择标准如表 4-10 所示。

表4-10 用户通过 IP 电话接入时园区网设备选择

序号	IP 语音用户数	建议选择部件
1	8 人以下	1、AR200 2、AR 1200，AR 1200 最高可以支持 32 路 SIP 语音用户
2	32 人以下	AR 1200，AR 1200 最高可以支持 32 路 SIP 语音用户
3	200 人以下	AR 2200，AR 2200 最高可以支持 512 路 SIP 语音用户
4	500 人以下	方案 1:AR2200，AR2200 最高可以支持 512 路 SIP 语音用户接入； 方案 2:AR3200, AR3200 最高可以支持 1024 路 SIP 语音用户接入

- 软终端接入

  通过在员工的 PC 上安装 SIP 软电话终端，通过连接在 PC 上的 MIC 和耳机实现企业员工的语音通信需求；同时，企业员工出差时，也可以通过 Internet 网络，将 SIP 软终端安装在出差 PC 机上，再注册到企业的 SVN 上，实现号码随人走不受工作地点的限制。

  WiFi 终端设备上可安装软件电话，提供园区内移动语音。

  软终端接入用户数量选择的标准同样参考上表 SIP 语音用户数量列表，与 IP PHONE 共享规格。

- 传真机接入

  企业将语音网络从传统的 PSTN 网络切换到 IP 网络时，企业原有的传统业务需要进行平滑过渡，企业的传真业务同时也需要在 IP 网络提供。企业在 IP 网络上提供传真业务，即路由器在其提供的 VoIP 服务功能的基础上加入 FAX 业务，因此用户只需花费低廉的费用就可以收发国际国内传真。

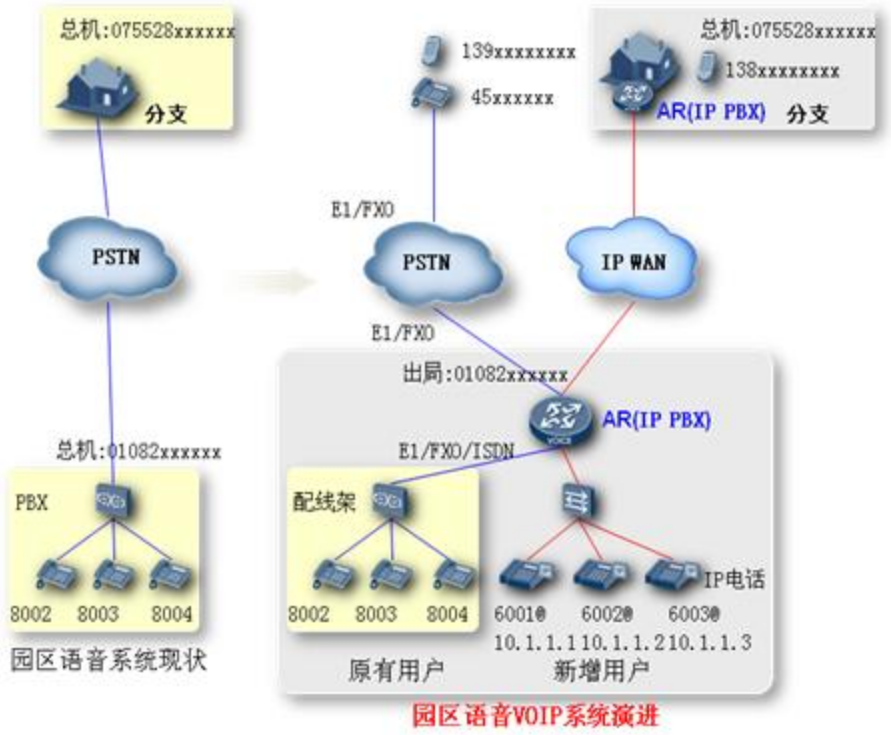
  基于 IP 网络的传真，主要有两种方式：存储转发传真和实时传真。

传统的传真机的接入通过传统的 RJ-11 电话线路接入，接入方式类似于模拟电话的接入方式，主要包括下面几种：

- 传真机通过 FXS 线路直接接到 AR 设备下；
- 传真机通过 FXS 线路接到 IAD 设备，IAD 设备通过以太链路接到 AR 设备下；
- 传真机通过 FXS 线路接到 TDM PBX 设备，TDM PBX 设备通过 E1 线路接到 AR 设备下。

- TDM-PBX 接入

图4-26 TDM-PBX 接入组网图



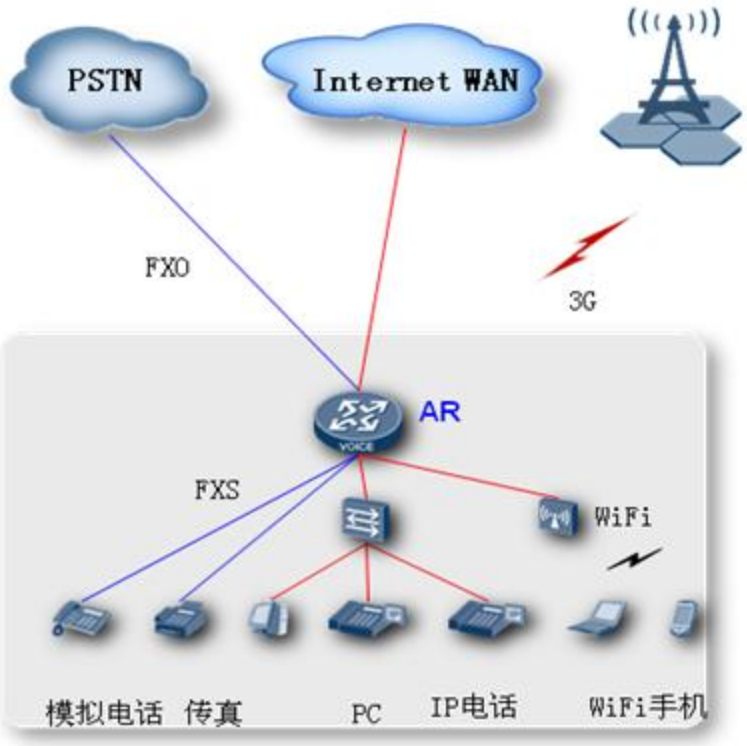
原有语音通信系统中有大量已有的投资，如 TDM PBX、POTS 话机，新建 IP 语音通信系统应充分考虑对原有投资的利用。

在园区出口部署 AR 系列路由器作为 IP PBX，通过 E1/FXO/ISDN 将原有 TDM PBX 接入到 AR，同时在 AR 路由器上配置 E1 或者 FXO 接口板，连接到本地 PSTN 网络，由 AR 管理出局呼叫路由及园区内部通话路由。

与其它分支园区之间的长途通话通过内部 IP 网络互通，AR 管理内部长途呼叫路由。

- 小型园区 ALL in ONE 接入

图4-27 小型园区 ALL in ONE 接入组网图



对于小型园区，AR 集成 3G、语音、路由功能，完成小型园区分支的统一接入。同时满足企业的数据业务、语音业务需求。

AR 作为 IP PBX，连接模拟和 IP 话机，实现基本语音功能，提供 IVR 等语音业务。AR 通过 FXO 口接入 PSTN 网络，实现与 PSTN 用户的通话。

WiFi 终端设备上安装软件电话，提供移动语音功能。

IP 地址规划

- AR

  AR 的以太 LAN 口 IP 地址需结合企业局域网规划和语音业务综合考虑。数据业务与语音业务部署到不同网段。

- IP 终端

  终端 IP 的分配方式有两种手段：

  - 通过静态配置，手工指定终端 IP。
  - 通过指定远端 DHCP Server 实现动态获取 IP。

号码规划

企业的号码规划一般有二种方式：DDI 方式和非 DDI 方式。

- DDI 方式下的企业号码规划，企业内部的每部电话都有一个长号，同时企业内部将长号的后四位或后五位做为每部电话的短号，企业内部的拔号直接通过短号互拔；同时，企业拔打公网语音用户，则通过拔打出局字冠+被叫号码进行出局形成出局

呼叫，而公网语音用户拔打企业语音用户时，可以直接使用企业语音用户的长号进行拔号通信。

- 非 DDI 方式下的企业号码规划，企业内部的每部电话分配一个短号，企业内部的拔号直接通过短号互拔；企业内部语音用户拔打公网语音用户时，通过 IP PBX 智能选择一个空闲的出局号码出局，而公网语音用户拔打企业语音用户时，外线先拔总机号码，再按照语音提示转发分机号码进行拔号通信。

路由规划

- IP PBX 的局内路由

  对于 IP PBX 管辖下的各个终端，在终端注册的时候，IP PBX 就已经获得了各终端的位置信息。因此，呼叫局内终端时不需要配置路由的，IP PBX 可以通过注册信息直接查找到目的终端的位置。

- IP PBX 的出局路由

  IP PBX 出局需要和对端 IPPBX 或者运营商网络对接，因为对端的终端信息在本地不可见，因此需要配置语音呼叫路由，用于分支间呼叫和外线呼叫。在大中型园区多分支场景中，建议总部 IP PBX 为各个分支互通提供呼叫路由，形成总部为一级呼叫路由，分支为二级呼叫路由的结构。这样的好处是新增一个分支，只需更改总部的配置，其他分支无需修改配置。

QOS 规划

语音是实时业务，对网络延迟、抖动很敏感，需要有较高的质量保证。在 TDM 时代，因为电路是独享的，语音质量可以自然得到保证。而在 VOIP 时代，使用以太网作为承载网络，需要为语音业务配置较好的质量保证。而语音质量的保证，重点在于承载网络为语音提供的 QoS。

承载网络为语音业务提供的 QoS，主要体现在业务优先级的识别。语音通话的特点是实时性要求高，延时小，呼叫接续快，因此语音的报文一般要求有较高优先级的转发，而路由器在做报文转发时是通过报文设置的 VLAN 优先级（遵循 802.1P）、DSCP/TOS 进行区分转发。

语音业务在二层以太网络中传送的时候,需要配置较高的 VLAN 优先级来保证语音业务质量，一般建议 VLAN 优先级配置为 6。华为公司的 IPPBX 设备使用专用的语音 VLAN 承载语音应用。语音 VLAN 自动为其承载的业务提供了较高的优先级保证，确保网络在拥塞的时候能够优先执行语音 VLAN 上的业务。

语音业务在三层 IP 网络中传送的时候，需要配置较高的 DSCP/TOS 优先级来保证语音业务质量。一般建议：如果 IP 网络选择 DSCP，则需要配置语音业务的 PHB 为“EF”（加速转发）；如果 IP 网络选择 TOS，则需要配置语音业务的优先级为 5。

一个完整的 QoS 端到端模型包括:IP 话机的 QoS 实现、PC 软终端的 QoS 实现、网络设备的 QoS 实现。

- IP 话机 QoS

  某些 IP 话机可以自行设置 QoS，建议对于信令流设置 DSCP 为 CS6，而媒体流设置 DSCP 为 EF。如果 IP 话机不能自行设置 QoS，则可以在接入设备上启用 VOICE VLAN 功能。

- POST 话机 QoS

POST 话机的 QoS 可以通过 IAD 实现。IAD 设备将 POST 话机的模拟信号转换为数字信号，并且给语音信令流和媒体流设置 DSCP 优先级。如果 IAD 不提供 DSCP 优先级设置，可在 IAD 接入的 AR 设备上启动 VOICE VLAN 功能。

- PC 软终端 QoS

  PC 机上对语音与数据流量不会加 802.1Q，一般情况下，对语音信令流和媒体流均设置高优先级的 DSCP 值，无论 PC 是有线接入还是无线接入，均需要在接入设备上根据入口报文的 DSCP 值进入相应的 DS 域，提高语音报文的优先调度转发，从而保证语音端到端 QoS 质量。

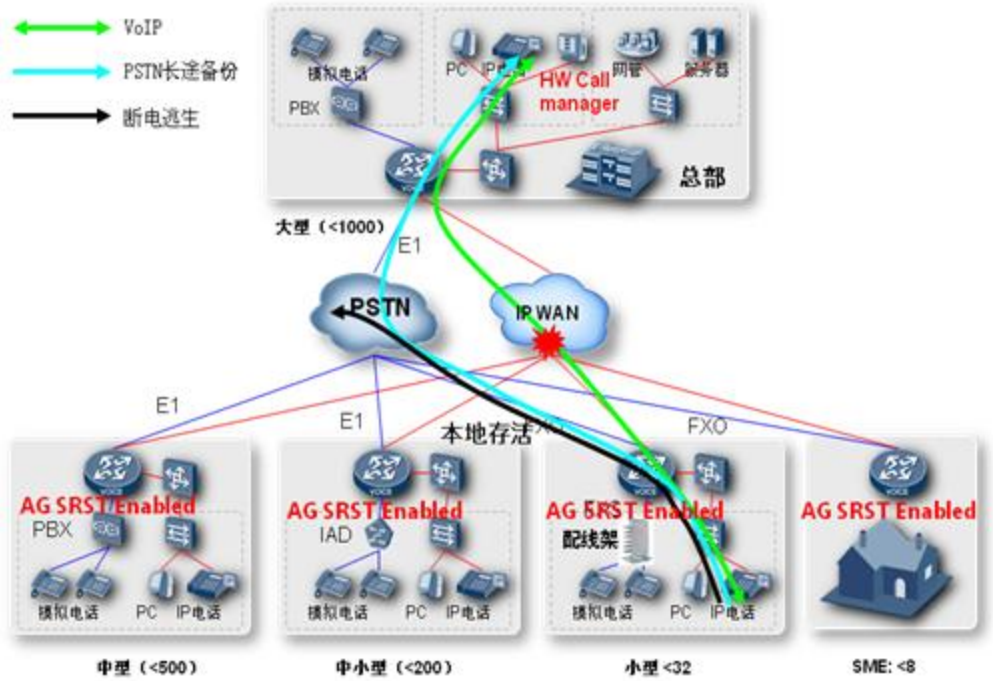
- 网络设备的 QoS

  整网中配置 DS 模型，接入交换机等网络设备根据入口报文的 DSCP 值或 802.1Q 值（从 DSCP 映射到 802.1Q）来识别语音流与数据流，并且提高语音报文的优先调度转发，从而保证语音端到端 QoS 质量。

可靠性规划

- 集中式呼叫控制场景可靠性规划

图4-28 集中式呼叫控制场景可靠性规划组网图



在集中式呼叫控制模式下，分支机构的 AG 及 IP phone 都注册到总部的 Call manager 接受呼叫控制。

使能 SRST 功能的 VG 检测到总部 Call manager 不可达的情况（WAN 链路故障或者 Call manager 不可达），启用本地存活（SRST），接管本分支 IP phone 及模拟话机的呼叫处理，并且 AR 可以通过绑定的 FXO/E1 拨打 PSTN，实现断网逃生。

AR（AG）通过 FXO 口连接到 PSTN，在设备断电或者故障情况下，FXS 口下挂的电话机转换为 FXO 接口电话线供电，接受运营商交换机馈电，共板卡 FXS 与 FXO

使 FXS 端口与 FXO 端口处于连通状态，实现断电逃生，保证用户摘机仍然能够拨打 PSTN 电话。

- 分布式多分支呼叫控制场景可靠性规划

  对于分布式控制方案，园区总部部署主备 IP PBX，总部的 IP 话机正常情况下注册在主用 IP PBX 上。当主用 IP PBX 故障，IP 话机切换注册到备用 IP PBX 上，切换后可以正常语音通话。

  下级园区部署到总部 IP PBX 的主备路由，正常情况下选择主用路由到达总部主用 IP PBX。

  分支 AR 设备作为 IP PBX，在 WAN 中断时，本级园区内呼叫可以本地存活。

  分支 AR 设备作为 IP PBX，在 WAN 中断时，本级园区可通过 PSTN 出口逃生。

语音业务部署

- 特色业务

  华为企业承载 IP 基础语音方案可以支持如下的特色业务，可以有效的解决和丰富企业的通信手段。

  - 一号通业务，通过配置一号通业务，将语音用户的座机号码、手机号码等一些电话号码绑定在同一个号。当用户成为被叫号码时，被叫用户的坐机号，手机号可以根据配置的规则进行同振或顺振，从而使被叫用户不会丢失每一次的业务呼叫；
  - 秘书业务，用户通过指定另一部电话来帮助处理其所有的来话呼叫，所有该用户的来话都将转移到秘书的电话上，并且只有秘书可以与其呼叫建立连接，从而由秘书屏蔽经理的所有来话业务。

- 基本业务和补充业务

  华为企业承载 IP 基础语音解决方案在提供上述特色业务的同时，也提供如下的基本业务和补充业务来完善企业语音用户的通信，更多业务请参考《VSP 业务操作手册》。

表4-11 基本业务和补充业务

基本业务	补充业务				
1 基本通话 2 传真业务 3 号码变换 4 智能路由 5 CDR 功能	主叫识别	呼叫保持	呼叫控制	群组业务	个性业务
	1 主叫号码显示 2 主叫号码显示限制	1 双通话业务 2 呼叫等待 3 呼叫转移 4 三方通话 5 呼叫前转	1 选择呼叫拒绝 2 选择呼叫接受 3 匿名呼叫拒绝 4 免打扰 5 呼叫拦截	1 同振 2 顺振 3 同组代答 4 指定代答 5 一机多号 6 IVR 排队	1 短号呼叫 2 区别振铃 3 缩位拨号 4 闹钟提醒 5 查号业务

4.3.5 语音管理维护

对于语音业务管理可以通过 eSight 统一进行管理，可实现功能如下：

- 语音质量监控方案，可以实现主动管理用户的语音网络
  - 通过 UDP Jitter 报文模拟语音报文检测语音质量，支持定时检测、阈值告警等。
  - 语音质量一目了然：时延、抖动、丢包，快速发现语音质量问题。
- 一键式内外线测试帮助用户管理语音线路问题

  模拟用户环路、模拟用户板等各项性能和指标（如线间电容、电阻、振铃、馈电、拨号音等）测试，由此判断是否出现断线、短路等故障，为用户语音线路维护提供参考。
- 批量号码发放，全面提升语音放号效率
  - 号码资源查询、统计管理。
  - 为 SIP 用户、POTS 用户分配号码。
  - 序列号码批量管理，全面提升语音放号效率。
  - 零星无规律号码批量配置：采用 Excel 导入等各种方式。

4.3.6 语音用户价值

园区语音通信从传统的接入运营商 PSTN 网络切换到 IP 网络，可以给用户带来如下的优势与体验价值：

- 企业用户通过企业内部的 IP 网络进行语音通信，企业内员工的长途话费与本地话费降到零，从而大大降低了企业的通信成本。
- IP 语音通信系统相对于传统的语音通信系统，可以很好的支持各种增值业务，从而丰富企业的通信手段， 如一号通业务，可以通过号码绑定，使客户不会错过任何一个商务电话。
- 将电话、传真、电话会议、即时消息、短消息等各种通信方式整合在一起，丰富了员工的通信手段，提高了员工的沟通效率。
- 企业的设备管理与维护统一、操作方便，降低企业的维护成本、提高工作效率。

4.4 视频监控业务承载方案

4.4.1 业务系统概述

视频监控业务系统主要包含如下五部分：

- 前端系统

  主要包括模拟摄像机（枪式、球型）、标清 IP Camera、高清 IP Camera、DVS/DVR、语音输入输出、报警输入输出等设备，主要实现前端音视频流和报警信息的采集及编码，提供给中心管理平台进行处理，是不可或缺的重要部分。
- 承载网络

  通过部署在各模块分局的 xPON 接入设备、编码设备、接入交换机、WIFI 实现所有前端监控点的直接接入。

  管理平台之间、管理平台与监控资源、用户终端之间通过视频监控专网进行信息的传输、交换和控制，能够有效地进行通信和共享数据，能够实现不同厂商、不同规格的设备或系统间的兼容和互操作。

- 中心管理平台

  网络监控系统中心平台部署在总部机房，是整个监控系统的核心，具有容量大、稳定性高，适应电信级应用，安全可靠。具备完善的主备方式、负载均衡机制，为接入大容量业务提供可靠性保证。

  管理平台采用分层分模块的设计方式，具有多级多域的逻辑结构。级数的设置和每一级所设域的数量可根据实际应用情况设置。

  软件采用模块化设计。对于不同的模块采用不同的专业应用部件。具体为：中心管理模块 SMC、业务控制模块 SCC、前端接入模块 PAG、客户端接入模块 CAG、媒体数据分发模块 MDU、媒体数据录像模块 MRU 等。切实满足视频监控业务对软件的需求。

- 存储系统

  存储管理分为媒体录像存储管理和数据库存储管理。

  媒体存储模块是针对视频监控录像文件的管理，通过提供文件管理储存功能，为客户提供按照文件分类管理文件，包括上传、支持批量上传、删除、支持批量删除、下载、查询文件列表的功能，以及添加、删除、修改、查询分类的操作功能和用户信息的管理（包括添加、修改、删除、查询用户信息）。

  媒体存储模块采用先进的存储技术，不宕机在线扩展容量、分块硬盘读写提供性能、校验冗余在个别磁盘失效的情况下仍然保持存储的可用、采用双电源、双控制器、双缓存、双风扇、热备热换等技术提供存储设备的可靠性，重要录像数据在总部中心自动备份转储，进行保存，以备授权后查询。同时支持故障告警、及时通知运维人员，尽快恢复故障设备。全方位的保障录像数据的可用、安全、可靠。

  数据库存储管理主要是针对视频监控中的核心业务数据，如用户信息、安全认证信息、系统运行参数信息等系统运行的核心业务数据。数据库数据采用镜像冗余存储备份，双机主备的访问方式，确保数据存储的核心数据安全可靠。

- 监控中心

  监控中心职能上分为总控中心、各分控中心及办公桌面软件客户端用户。逻辑上构建成一个多层次的网络监控系统，各级监控中心通过部署监控主机、解码器、显示系统及系统中心平台客户端软件，依托系统中心平台的全局管理功能实现对前端监控点的图像管理、存储管理、设备管理、告警管理。

  通过建设 DLP 大屏拼接系统实现对对监控演示中心的情况控制、突发事件的处理、事件查看、信息发布、监控调用、设备控制等功能的实现直接的大屏幕显示，实现对上述功能事件、功能系统、设备系统进行最直接最有效的点对点控制。

  视频监控系统可提供基于 IP 网络的图像远程监控、传输、存储、管理业务，其优点在于系统能利用无处不在的网络，将分散、独立的图像采集点进行联网，实现跨区域统一监控、、统一存储、统一管理及资源共享。

本方案只涉及视频监控业务在金融企业园区网络上的承载。

4.4.2 金融园区网视频监控承载方案

华为金融园区视频监控承载方案设计主要需要考虑摄像头的接入方式、视频数据流的传输、以及网络各节点所需带宽这三个方面，从而进行具体网络设计以及设备选型。

摄像头接入方案

- 摄像头类型

前端摄像头分为标清（720P）、高清（1080P）等不同清晰度的设备，可根据需要部署，一路标清视频大约 2M，一路高清视频大约 4~8M； 数字摄像头可以直连百兆接入；模拟摄像头需要经 DVS/DVR 进行数模转换然后再千兆接入；模数混合时，模拟摄像头经过编码器千兆接入；摄像头进行数据采集并实时上传，网络要求低延时。

常见不同分辨率的摄像头所需带宽如下表：

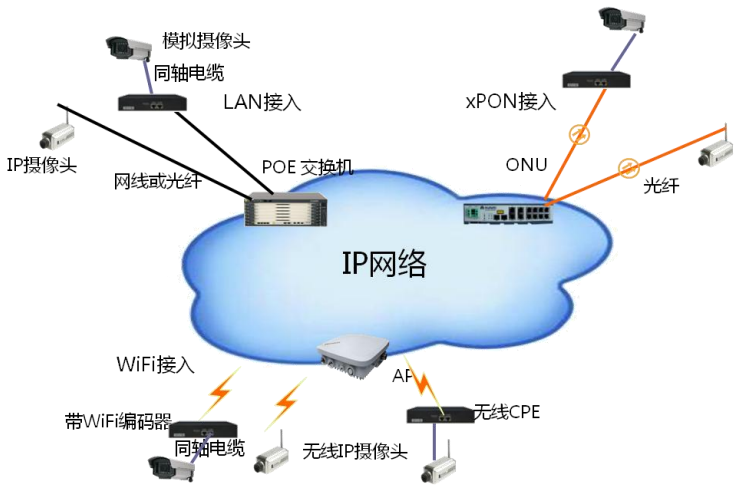
表4-12 不同分辨率的摄像头所需带宽

分辨率	CIF (352×288)	4CIF (704*576)	720P (1280*720)	1080P (1920*1080)
带宽要求	384~512kbps	512~2048kbps	2Mbps~4Mbps	4Mbps~ 8Mbps
帧速率	15~20fps	20~25fps	20~30fps	35fps
画质	Normal	Good	Better	Excellent

- 接入方案

  华为金融园区视频监控承载方案提供多种接入方式，满足不同场景的视频监控需求，使接入更灵活方便。

图4-29 接入方案



交换机接入：适合金融园区、商业楼宇内易于布线的室内视频监控接入场景；可以根据摄像头分布密度选取树型、星型、环型等组网方式；

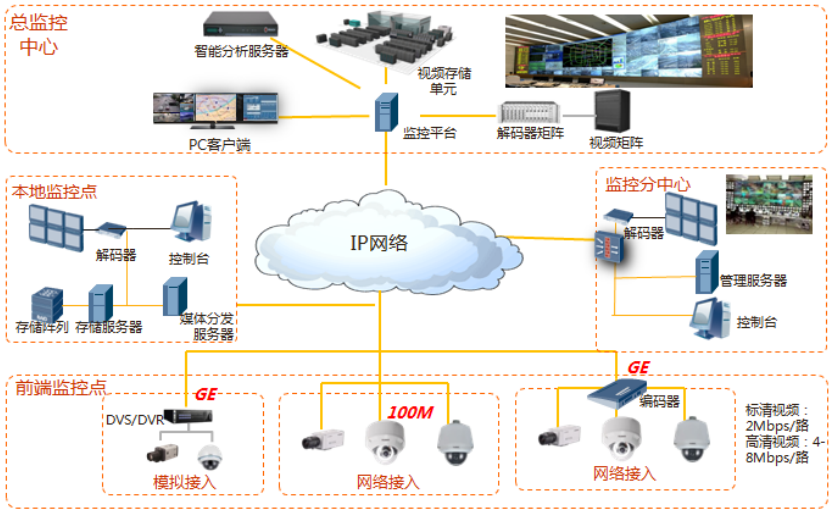
WIFI 接入：适合园区内布线不方便的室外监控场景 ；

xPON 接入：适合线型区域覆盖、园区道路、室外接入场景，能够支持较长传输距离。

实际方案设计中，需根据摄像头分布密度以及现场场景选择合适接入方式。

视频监控数据流向分析

图4-30 进入园区网视频监控业务系统架构示意图



如图 4-30 视频监控业务系统架构示意，园区视频监控流量主要有以下四种：

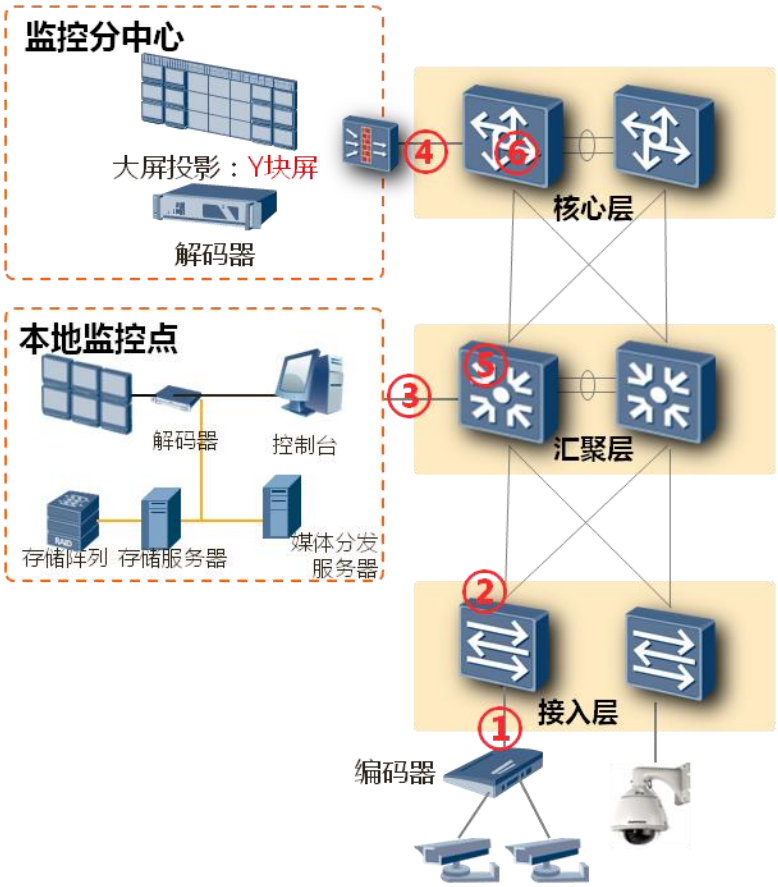
- 前端监控点到本地监控中心以视频单播流量为主；视频流经由媒体分发器后分为两路：一路存储，一路经由解码器由监控大屏实时显示；
- 去往分中心流量：由视频采集前端设备通过单播或组播方式传递的实时视频流、视频存储流以及分中心内部的单播视频回放流；
- 去往监控总中心流量：由视频采集前端设备通过单播或组播方式传递的实时视频流、视频存储流以及总中心内部的视频回放流；
- 存储服务器到后端存储中心的视频备份流量一般通过独立 SAN 存储网络传输。

当采用组播方式时，局域网环境内，将连接组播来源与目地的交换机端口启用 IGMP 协议以优化组播包传递效率。

对于不支持组播的网络，实时视频流也可以通过媒体服务器进行复制转发，网络部署简单，易实现。

视频监控传输带宽计算示例

图4-31 金融园区网视频监控传输带宽计算示例图



视频监控网络内实际流量与摄像头数目、分布、使用的分辨率以及监控中心部署的位置和层次结构有关，无法给出统一的计算公式。此处仅如上图所示按照接入汇聚核心经典三层组网结构，进行传输带宽计算示例。

其中，假设单摄像头视频数据流峰值带宽为 N，每块屏最大支持 M 路实时视频输入。

网络各节点带宽计算方法：

①单编码器总峰值流量=N*摄像头数量

②单接入交换机峰值流量=N*接入摄像头数量

③本地监控点：峰值流量=N*本地摄像头数量

④监控分中心：实时视频峰值流量=N*M 路*Y 块屏

⑤汇聚交换机最大需要处理的流量包括：该汇接区域视频存储流和监控分中心实时视频流=③+④

⑥此处核心交换机最大需要处理的流量等于到监控总中心的实时视频流量=④

各节点设备选型需根据网络各节点带宽，并保证一定带宽冗余，建议流量占设备总带宽15%~50%，具体根据项目成本和业务扩展需求确定，具体设备选型此处不再赘述。

5 设备说明

5.1 华为全系列交换机

5.1.1 S9700 系列高性能核心路由交换机

Quidway®S9700 系列运营级核心交换机是由华为公司自主开发的新一代高性能核心路由交换机产品，为满足多种业务在城域以太网上高质量的传输，。S9700 主要应用于城域网中的业务接入、汇聚和传输层，作为城域网的接入和汇聚节点，提供线速的 FE、GE 和 10GE 接口，同时可提供 155M、622M 和 2.5G 的 WAN 接口。也可以应用于行业网、数据中心，提供高密度的端口和丰富的增值业务能力。

表5-1 S9700 系列交换机

产品型号	设备外观图	说明
S9703		交换容量 2.88Tbit/s 背板容量 7.2Tbit/s 转发能力 1440Mpps

产品型号	设备外观图	说明
S9706		交换容量 3.84/5.76Tbit/s 背板容量 14.4Tbit/s 转发能力 2880/4320Mpps
S9712		交换容量 3.84/5.12/7.68Tbit/s 背板容量 19.2Tbit/s 转发能力 2880/3840/5760Mpps

S9700 系列产品有如下特点：

- 灵活的扩展能力

  供电能力：目前系统电源 AC 模块的最大供电能力为 2200W，DC 模块的最大供电能力是 2200W，支持 M+N AC/DC 电源备份。

- 强大的转发能力

  S9700 产品实现组播线速转发，硬件完成两级复制：交换网板复制到接口板和转发引擎复制到接口。

- 丰富的业务性能

- 提供丰富的二层业务特性，主要特性包括：VLAN、GARP/GVRP、灵活 QinQ、RRPP、SEP、Smartlink、STP/RSTP/MSTP、DHCP snooping、IGMP snooping、MLD snooping、Ethernet OAM；
- 提供丰富的IP业务特性，包括IPv4 和IPv6单播路由协议、组播路由协议、VRRP、DHCP Relay/ DHCP Server/Option82 等；
- 全面支持 MPLS 业务，主要包括：MPLS 转发、LDP、MPLS-TE、MPLS-OAM；
- 提供完善 VPN 业务，主要特性包括：VPLS、VLL、BGP/MPLS IP VPN;
- 支持防火墙/NAT；
- 支持负载均衡；
- 支持 IPSec VPN。

- 周密的安全设计

  S9700产品确保了数据平面和控制平面之间的自然分离，提供业界领先的安全性能。

- 电信级的可靠性

  S9700 产品的整机结构还提供了功能强大的监控系统。通过独立的监控单元实现对整个系统的管理维护。实现对单板、风扇和电源配电模块的管理、监控和维护。

  S9700 产品完全满足 EMC（Electro Magnetic Compatibility）要求。系统采用模块级屏蔽，实现了单板间的 EMC 隔离。

- 良好的可维护性

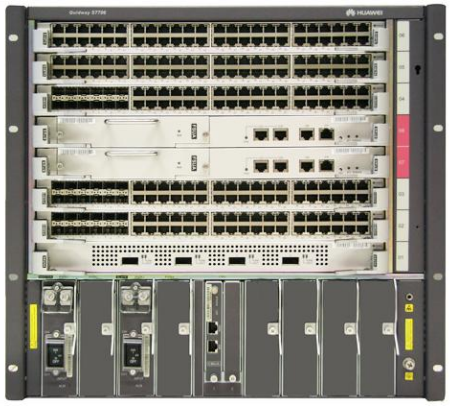
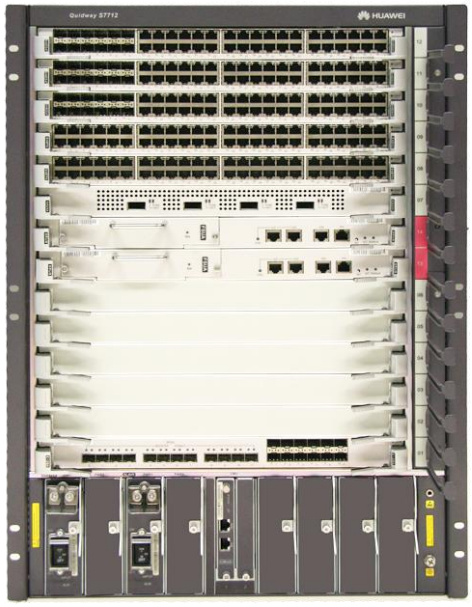
  支持以太网 OAM；支持 MPLS OAM 能力；支持端到端的 OAM；支持基于物理端口、VLAN、LSP、ACL 的流量统计；支持 eSight 管理；支持远程设备维护功能；支持热补丁功能；支持版本回退功能。

5.1.2 S7700 系列高性能核心路由交换机

Quidway®S7700 系列运营级园区汇聚交换机是由华为公司自主开发的新一代高性能核心路由交换机产品，提供大容量、高密度、模块化的二到四层线速转发性能，具有强大组播功能，完善的 QoS 保障、有效的安全管理机制和电信级的高可靠设计，满足高端用户对多业务、高可靠、大容量、模块化的需求，降低运营商的建网成本和维护成本，可广泛应用于构建各种类型型园区网核心层和汇聚层交换机。

表5-2 S7700 系列交换机

产品型号	设备外观图	说明
S7703		支持 3 块 LPU 交换网容量 288Gbit/s 背板容量 1.2Tbit/s 转发能力 215Mpps

产品型号	设备外观图	说明
S7706		支持 6 块 LPU 交换网容量 1.536Tbit/s 背板容量 2.4Tbit/s 转发能力 432Mpps
S7712		支持 12 块 LPU 交换网容量 1.536Tbit/s 背板容量 4.8Tbit/s 转发能力 864Mpps

S7700 系列产品有如下特点：

- 先进体系结构，高性能，配置灵活
  - S7700 系列交换机采用先进的全分布式体系结构设计，采用业界最新的硬件转发引擎技术，所有端口支持的业务能够线速转发，业务包括 IPv4/MPLS/二层转发等。支持 ACL 线速转发。
  - S7700 系列交换机实现组播线速转发，硬件完成两级复制：交换网板复制到接口板和转发引擎复制到接口。
  - S7700 支持 1.536Tbps 交换容量，支持多种高密度板卡，满足核心、汇聚层设备大容量、高端口密度的要求，可以满足用户日益增长的带宽需求，能够极大的保护和节约用户投资。
- 完善的安全机制
  - S7700 系列交换机支持 OSPF、RIP v2 及 BGP v4 报文的明文及 MD5 密文认证，支持安全的 SSH 登录、命令行分级保护、基于用户安全策略的 SNMP V3、DHCP

Snooping、IP Source Guard、DAI、层次化 CPU 通道保护，并提供以下几种用户认证方式：本地认证、RADIUS 和 HWTACACS 认证。

- 支持防网络风暴攻击、防 DOS/DDOS 攻击、防扫描窥探攻击、防畸形报文攻击、防网络协议报文攻击等安全技术。

- 全面的可靠性
  - S7700 系列交换机最大支持 128 个汇聚组，每个汇聚组内支持最多 8 个成员端口，支持跨单板端口间的汇聚。
  - 支持 DLDP，可以监控光纤或铜质双绞线的链路状态。如果发现单向链路存在，DLDP 会根据用户配置，自动关闭或通知用户手工关闭相关端口，以防止网络问题的发生。
  - 支持 RRPP 及多实例，相比其他以太环网技术，RRPP 具有以下优势：拓扑收敛速度快，低于 50ms。收敛时间与环网上节点数无关，可应用于网络直径较大的网络。
  - 支持标准 STP/RSTP/MSTP 二层环网保护协议。
  - 支持 SmartLink 及多实例。
  - 支持 BFD for 单播路由/VRRP/FRR/PIM。

5.1.3 S5700 系列以太网交换机

Quidway®S5700 系列以太网交换机（简称 S5700）是华为公司推出的集接入、汇聚和传送功能于一身的以太网交换机，满足企业网对多业务可靠接入和高质量传输的要求。

S5700 定位于企业网多业务的接入汇聚层，具有大容量、高密度、高性价比的分组转发能力。借助 S5700 可构建高可靠的环网拓扑，具有多业务接入能力、良好的扩展性、QoS、强大的组播复制能力和运营级的安全性。

表5-3 S5700 系列交换机

产品型号	设备外观图	备注
S5700-28C-EI		三层交换机 下行 24 个 GE 电 上行支持三种插卡 1、4 个 XGE 光 2、2 个 XGE 光 3、4 个 GE 光 增强三层功能

产品型号	设备外观图	备注
S5700-28C-EI-24S		三层交换机 下行 24 个 GE 光 上行支持两种插卡 1、4 个 XGE 光 2、2 个 XGE 光 3、4 个 GE 光 增强三层功能
S5700-52C-EI		三层交换机 下行 48 个 GE 电 上行支持两种插卡 1、4 个 XGE 光 2、2 个 XGE 光 3、4 个 GE 光 增强三层功能
S5700-24TP-SI	DC  AC 	三层交换机 24 个 GE 电 基本三层功能
S5700-24TP-PWR-SI		三层交换机 24 个 GE 电 基本三层功能 支持 PoE
S5700-48TP-SI		三层交换机 48 个 GE 电 基本三层功能
S5700-48TP-PWR-SI		三层交换机 48 个 GE 电 基本三层功能 支持 PoE

产品型号	设备外观图	备注
S5700-28C-PWR-EI		三层交换机 下行 24 个 GE 电 上行支持两种插卡 1、4 个 XGE 光 2、2 个 XGE 光 3、4 个 GE 光 增强三层功能 支持 PoE
S5700-52C-PWR-EI		三层交换机 下行 48 个 GE 电 上行支持两种插卡 1、4 个 XGE 光 2、2 个 XGE 光 3、4 个 GE 光 增强三层功能 支持 PoE
S5700-28C-SI		三层交换机 下行 24 个 GE 电 上行支持两种插卡 1、4 个 XGE 光 2、2 个 XGE 光 3、4 个 GE 光 基本三层功能
S5700-52C-SI		三层交换机 下行 48 个 GE 电 上行支持两种插卡 1、4 个 XGE 光 2、2 个 XGE 光 3、4 个 GE 光 基本三层功能

S5700 系列交换机的特点是：

- 电信级的可维护性
  - S5700 遵循电信级标准设计，风扇、电源可现场更换，方便维护；机箱重量轻，可以安装在 600mm 深机柜中，且安装方便。

- S5700 提供软件热补丁技术，实现设备软件在线平滑升级。
- S5700 支持快速保护倒换机制 RRPP（Rapid Ring Protection Protocol），可以快速实现链路级和业务级保护倒换，满足运营级的可靠性要求。

- 强大的多业务接入能力
  - S5700 通常部署在企业网的汇聚层，可直接接入来自下游 AMG（Access Media Gateway）和 LSW（LAN Switch）等设备的业务，并汇聚到上游设备。可接入的业务包括：VoIP、IPTV/VOD（Video On Demand）视频业务以及宽带上网业务。
  - S5700 采用成熟、经济的 IP 内核技术，借助高性能 ASIC（Application Specific Integrated Circuit）芯片，提供大容量的数据交换能力，满足传统电信业务对低时延抖动、高可靠性的需求。S5700 采用以太网组网技术，支持组播业务，提供良好的 QoS 机制和多种保护倒换技术，实现了良好的带宽保证和多业务支持能力。
- 灵活的组网能力
  - S5700 提供 10/100/1000BASE-T 以太网电接口、100/1000BASE-X 以太网光接口及万兆以太网光接口，支持 Access、Trunk 和 Hybrid 等多种接口类型。
  - 对于千兆光纤连接，S5700 提供可插拔的 SFP（Small Form-Factor Pluggable）类型光模块。对于万兆光纤连接，S-switch 提供可插拔的 XFP（10Gigabit SmallForm Factor Pluggable）和 SFP+（SmallForm-Factor Pluggable Plus）类型光模块。光纤长度可以根据用户对传输距离的需求灵活选配。
  - S5700 可以组成树状、星型和环状以太网。对于环状以太网，S5700 提供 STP（Spanning Tree Protocol）和 RRPP，消除环路并提供快速保护倒换。
- 网络级 QoS 保障

  S5700 具备完善的 QoS 机制。S5700 能够智能感知业务，能够对 OSI 模型 2～4 层信息进行流分类，根据流分类结果提供访问过滤、流量监管、队列调度策略，从而确保不同业务对差别服务的要求。
- 多层面的扩展能力
  - S5700 以华为公司拥有自主知识产权的 VRP（Versatile Routing Platform）平台为基础，结合设备和网络管理技术，提供高速的交换能力和丰富的业务特性。
  - S5700 支持灵活业务插卡和多功能插槽，满足未来业务的扩展需求。
- 周密的安全措施

S5700 保障设备和数据传输的安全，有效的防止恶意用户对网络的攻击。

- 支持基于 MAC 地址的过滤。
- 提供丰富的 ACL 策略。
- 提供“VLAN＋MAC”的查表机制。
- 支持流量抑制。

S5700 提供安全的用户登录操作保护。

- 对登录用户提供口令保护，口令可加密功能。
- 通过配置用户级别和命令级别实现对命令的分级保护。
- 通过命令锁定当前配置终端，防止设备被非法使用。
- 对影响系统性能的重要命令，提供确认和提示。

S5700 提供 ALS（Automatic Laser Shutdown）功能，在光纤连接断开时停止发送激光，有效避免激光对用户的伤害。

- 便捷的操作维护

  S5700 不仅自身提供基于接口的流量统计功能，支持 IP 网络中 Ping、Tracert 等故障检测和定位技术。而且还能配合华为公司 eSight 企业网络管理系统，提供丰富的性能监视、告警和快速的故障定位能力。

  S5700 还支持基于 GUI 的 Web 网管界面，为用户提供友好的配置和管理界面。通过 Web 网管，用户可以很方便的通过 GUI 界面管理设备，降低对初级维护人员的要求。

  此外，S5700 还支持 HGMP（Huawei Group Management Protocol）集群管理，通过自动收集设备拓扑的方法以及集中的维护管理通道，使一台设备可以管理多台二层交换机。

- 绿色节能设计

S5700 采用多种节能措施，包括：

  - 采用静音风扇，风扇转速自动调整，降低系统的噪音，节省风扇功耗。
  - 当检测不到业务端口对端连接设备，即端口空闲，则芯片进入省电模式，以减小功耗。
  - 采用先进工艺、高集成度、低功耗芯片，并配合智能设备管理系统充分利用芯片的低功耗特性，在提升系统性能的同时还降低了整机功耗。

- 先进的防雷技术

  S5700 采用华为专利内置防雷技术，可以应对各种恶劣环境，如架空走线。从而降低设备在雷击天气中的损坏概率，大大提高设备可靠性，将安全系数提高 30 倍。

- 人性化的 PoE 供电方式

  S5700 支持 PoE（Power over Ethernet）功能，即可以通过双绞线向远端下挂的 IP 电话、无线 AP(Access Point)、便携设备充电器、刷卡机、摄像头、数据采集等终端设备提供集中式的电源供电，降低用户的初期投资成本。

  S5700 支持 802.3af 标准和 802.3at 标准，解决不同厂家设备远端供电问题。其中，802.3at 标准支持最大 30W 的供电能力，可以为新一代的 IP 可视电话、双频 WiFiAP，视频监控摄像机，多功能 STB11，RFID 读卡器等大功率设备提供电力，降低网络复杂度。

  S5700 提供基于时间段的供电控制能力，有效管理网络设备和电力消耗，降低运营成本。

5.1.4 S3700 系列以太网交换机

Quidway®S3700 系列以太网交换机（简称 S3700）是华为公司推出的集接入、汇聚和传送功能于一身的以太网交换机，满足企业网对多业务可靠接入和高质量传输的要求。

S3700 定位于企业网多业务的接入汇聚层，具有大容量、高密度、高性价比的分组转发能力。借助 S3700 可构建高可靠的环网拓扑，具有多业务接入能力、良好的扩展性、QoS、强大的组播复制能力和运营级的安全性。

表5-4 S3700 系列交换机

产品型号	设备外观	备注
S3700-28TP-SI	AC  DC 	三层交换机 下行 24 个 FE 电 上行 2 个 GECombo 和 2 个 GE 光 基本三层功能
S3700-28TP-EI		三层交换机 下行 24 个 FE 电 上行 2 个 GECombo 和 2 个 GE 光 增强三层功能
S3700-28TP-EI-24S		三层交换机 下行 24 个 FE 光 上行 2 个 GECombo 和 2 个 GE 光 增强三层功能
S3700-52P-SI		三层交换机 下行 48 个 FE 电 上行 4 个 GE 光 基本三层功能
S3700-52P-EI		三层交换机 下行 48 个 FE 电 上行 4 个 GE 光 增强三层功能
S3700-52P-EI-24S		三层交换机 下行 24 个 FE 光和 24 个 FE 电 上行 4 个 GE 光 增强三层功能
S3700-52P-EI-48S	AC:  DC: 	三层交换机 下行 48 个 FE 光 上行 4 个 GE 光 增强三层功能

产品型号	设备外观	备注
S3700-28TP-PWR-EI		三层交换机 下行 24 个 FE 电 上行 2 个 GECombo 和 2 个 GE 光 增强三层功能 支持 PoE
S3700-52P-PWR-EI		三层交换机 下行 48 个 FE 电 上行 4 个 GE 光 增强三层功能 支持 PoE
S3700-28TP-EI-MC		三层交换机 下行 24 个 FE 电 上行 2 个 GECombo 和 2 个 GE 光 增强三层功能 支持监控和掉电告警

由于采用相同的软件平台，S3700 在软件功能特性方面和 S5700 基本一致，在此不再重复。下面主要介绍一下 S3700 与 S5700 不同的特点：

- 电信级可维护性方面，S3700 机箱采用前向维护结构，方便日常操作和维护。
- 灵活组网方面，S3700 提供 10/100BASE-T 以太网电接口、10/100/1000BASE-T 以太网电接口和 100/1000BASE-X 以太网光接口（S5700 支持万兆以太网接口）。
- 绿色节能设计方面，S3700-28TP-SI/EI 采用自然散热，无噪声污染，产品可靠性高；节省风扇功耗，并避免定期维护风扇，节省维护费用；无风扇等额外功耗，使产品达到更好的能效功耗比；还可以有效的避免单板腐蚀。

5.1.5 S2700 系列以太网交换机

Quidway®S2700 系列以太网交换机（简称 S2700）是华为公司推出的集接入和传送功能于一身的以太网交换机，满足企业网对多业务可靠接入和高质量传输的要求。

S2700 定位于企业网多业务的接入层，具有大容量、高密度、高性价比的分组转发能力。借助 S2700 可构建高可靠的环网拓扑，具有多业务接入能力、良好的扩展性、QoS、强大的组播复制能力和运营级的安全性。

表5-5 S2700 系列交换机

产品型号	设备外观	备注
S2700-9TP-EI	AC  DC 	以太网交换机 下行 8 个 FE 电 上行 1 个 GECombo 支持 ACL
S2700-9TP-SI		以太网交换机 下行 8 个 FE 电 上行 1 个 GECombo
S2700-18TP-EI		以太网交换机 下行 16 个 FE 电 上行 2 个 GECombo 支持 ACL
S2700-18TP-SI		以太网交换机 下行 16 个 FE 电 上行 2 个 GECombo
S2700-26TP-EI	AC  DC 	以太网交换机 下行 24 个 FE 电 上行 2 个 GECombo 支持 ACL
S2700-26TP-SI		以太网交换机 下行 24 个 FE 电 上行 2 个 GECombo
S2700-52P-EI		以太网交换机 下行 48 个 FE 电 上行 4 个 GE 光 支持 ACL
S2700-9TP-PWR-EI		以太网交换机 下行 8 个 FE 电 上行 1 个 GECombo 支持 ACL 支持 PoE

产品型号	设备外观	备注
S2700-26TP-PWR-EI		以太网交换机 下行 24 个 FE 电 上行 2 个 GECombo 支持 ACL 支持 PoE

由于采用相同的软件平台，S2700 在很多软件特性上与 S3700 基本一致，最大的不同在于 S2700 为二层交换机，因此不具有三层相关的特性和功能，而 S3700 同时支持二层和三层的硬件线速转发。在硬件设计上，S2700 大部分型号采用自然散热的无风扇设计，包括 S2700-9TP-PWR-EI、S2700-9TP-SI/EI、S2700-18TP-SI/EI、S2700-26TP-SI/EI 等。

5.2 AR 系列路由器

Quidway®AR12/22/32 系列路由器是华为公司为满足新一代企业分支、中小企业的 WAN 接入和运营商转售市场多业务承载需求而推出的新一代接入路由器产品。

AR12/22/32 系列路由器基于新一代高性能硬件和华为公司统一的 VRP 软件平台，支持丰富的广域网接口，提供高密度以太、语音等用户接入，支持 IPSec VPN 和防火墙等安全功能，可充分满足企业分支互联、中小企业广域接入和运营商转售等多种场合的需求。

Quidway®AR12/22/32 分为 AR12、AR22 和 AR33 三个系列产品。

表5-6 AR 系列产品

产品型号	设备外观	备注
AR1220		整机容量：8Gbps 转发性能： 350Kpps/200Mbps(64byte)
AR1220V		整机容量：8Gbps 转发性能： 350Kpps/200Mbps(64byte)
AR1220W/1220VW		整机容量：8Gbps 转发性能： 350Kpps/200Mbps(64byte)
AR2220		整机容量：32Gbps 转发性能： 1Mpps/500Mbps(64byte)

产品型号	设备外观	备注
AR2240		整机容量：80Gbps 转发性能：2Mpps/1333Mbps(64byte)
AR3260		整机容量：160Gbps 转发性能：3.5Mpps（SRU80高性能主控板）/2000Mbps(64byte)

AR 系列产品的特点如下：

- 高性能

  华为 AR 产品采用最新的 ASIC 芯片和多核 CPU。LAN 模块内接口之间线速转发，LAN 模块之间具有高带宽 Fabric。CPU 采用 500MHz 两核到 750MHz12 核的 MIPS 处理器，25M 到 1G 的 WAN 转发性能，CPU 内置高性能加解密模块，具有 25M 到 300M 的加解密性能。

- 多业务集成

  华为 AR 产品除了提供对数据业务的支持外，还可以同时作为 IP PBX、IPSec VPN 网关和防火墙使用，AR12 还有支持 WLAN AP 的型号，真正做到数据、语音、视频、安全、无线等多业务的统一集成。

- 强大的 QoS

  华为 AR 产品支持 3 级 HQoS，其中 3260 通过 TM 硬件提供更强的转发性能。

- 高密度接入

  华为 AR 提供高密度的语音和数据接入，通过不同类型的插卡组合，可以充分满足各种场景下语音和数据的混合接入。

- 丰富的广域网接口

  华为 AR 提供丰富的广域网接口，包括 E1/T1、ISDN BRI、FR、3G 等各种主流接口，并支持作为 MPLS VPN 的 CE 和 PE 设备。

5.3 华为 NE 系列路由器

5.3.1 NE40E 系列

HUAWEI Net Engine40E 全业务路由器，简称 NE40E，是华为公司推出的高端网络产品，主要应用在各种大型园区网的边缘位置。

NE40E 的操作系统采用功能强大的通用路由平台 VRP，具有业务丰富、超大容量、高性能和高可靠性的特点。

表5-7 NE40E 系列路由器

产品型号	设备外观	备注
NE40E-X16		交换容量：2.56T 转发性能：1600Mpps
NE40E-X8		交换容量：1.44T 转发性能：800Mpps
NE40E-X3		交换容量：1.08T 转发性能：300Mpps

产品型号	设备外观	备注
NE40E-8		交换容量：640G 转发性能：400Mpps
NE40E-4		交换容量：320G 转发性能：200Mpps

NE40E 系列产品的特点如下：

- 400G 平台，满足未来十年的发展需求
  - 设备紧凑，端口密度大，最高密度 1320GE/机框。
  - 绿色的 400G 平台，大容量低功耗。
  - 兼容设计，从 40G 升级到 400G 平台，单板、软件完全兼容。
- 全业务承载业界领先，为电信级业务运营保驾护航
  - 支持 BRAS、DPI 等功能模块，保证多业务接入能力。
  - 完整的 HQoS 解决方案，HQoS、DS-TE 和 MPLS HQoS，保证多场景的 QoS 部署。
  - 领先的增强视频解决方案，实现 FCC、RET、iRSM、iVSE 等技术，增强用户视频体验。

- 完善的端到端可靠性解决方案，保证业务永不中断
  - 设备级可靠：关键部件冗余备份，配合 ISSU/NSR/GR 等技术，最大限度避免业务中断运行。
  - 网络级可靠：华为独有的 BFD For anything、E-系列等技术，保证业务端到端 200ms 保护倒换。
  - 业务级可靠：业界领先的 BRAS Pool 解决方案，保证视频等高端业务永远在线，增强用户体验。

5.3.2 NE20E 系列

NetEngine20E/20 系列路由器（以下简称 NE20E/20）是华为公司自主研发的通用高性能第五代多业务路由器。NE20E/20 采用 NP 硬件技术实现，具有卓越的转发性能。

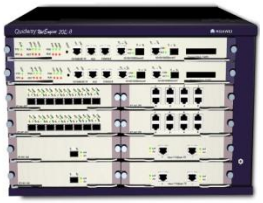
NE20E/20 系列路由器旨在满足企业网汇聚和运营商边缘的电信级高可用性的要求。以其高性能、多业务、双主控和热备份优势，进行业务运营和支撑网络的建设。NE20E/20 具有很强的可伸缩性、可配置性，支持多种接口和业务特性，将 MPLS、VPN、QoS、流量工程、组播等技术融合起来。

在组网应用方面，NE20E/20 系列路由器作为高性能汇聚设备提供全面的业务处理能力，提供全方位的、灵活的网络解决方案，有效提高了网络价值并节约了网络建设成本。

NE20E/20 系列路由器按业务槽位数可分为 NE20E-8、NE20-8、NE20-4、NE20-2 四款产品，NE20E 是 NE20 的增强型产品。

NE20E/20 系列的产品型号如下：

表5-8 NetEngine40E 核心路由器系列产品型号

产品型号	设备外观图	描述
NE20E-8		支持8块LPU 交换网容量16Gbps（双向） 转发能力6Mpps
NE20-8		支持8块LPU 交换网容量8G（双向） 转发能力4.5Mpps
NE20-4		支持4块LPU 交换网容量 8G（双向） 转发能力 4.5Mpps

产品型号	设备外观图	描述
NE40-2		支持2块LPU 交换网容量8G（双向） 转发能力3Mpps

NE20E 系列产品的特点如下：

- 稳定成熟应用

  NE20E/20 是多年成熟稳定应用的经典路由器。
  - 大规模成熟商用 8 年，全球发货 10000 余套。
  - 多年零质量事故，表现优异。
- 多业务接入和汇聚能力

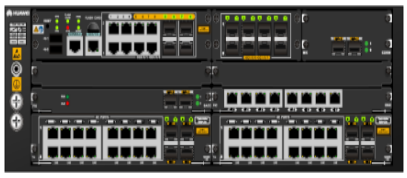
  NE20E/20 是全系列多业务产品，可灵活满足企业客户需求。
  - 强大的汇聚能力，ATM、CPOS、CE1 等接口线速汇聚（可汇聚 96 个线速 E1/T1）。
  - 强劲的安全隧道能力，IPSec 硬件加密，GRE、L2TP、NAT 性能灵活优异。
  - 全面的路由处理能力，全面支持各种单播和多播路由协议。
- 高可靠性

  NE20E/20 提供完善的端到端可靠性解决方案，可保证业务不中断。
  - 业界首款控制引擎与转发引擎双备份设备，提供高品质业务保障。
  - 设备级、网络级、业务级全方位的可靠性技术，保证网络运行高速可靠。
  - 层次化的 HQoS，灵活保障业务质量。

5.4 防火墙产品系列

E1000E-X 系列防火墙采用万兆多核全新硬件平台，轻松实现海量业务处理，打造业务永续的办公网络；融合 Symantec 先进的入侵防御和反病毒技术，重新演绎专业内容安全防御，营造更安全的办公网络；集成华为业界领先的 DPI 识别技术，精细管理超千种应用程序，创建更高效的办公环境。

表5-9 防火墙系列产品

产品型号	设备外观	备注
E1000E-U2		4 个 GE 光电互斥接口、1 个 Console 口、2 个 USB 口； 2 个扩展槽； 支持 2GE、4FE 接口板； 吞吐量：2Gbps；
E1000E-U3		固定接口：4GE 电+4GECombo 支持万兆接口 标配双电源(AC/DC 可选) 扩展槽：2*FIC 吞吐量：6Gbps
E1000E-U5		固定接口：4GE 电+4GECombo 支持万兆接口 标配双电源(AC/DC 可选) 扩展槽：2*FIC 吞吐量：10Gbps
E1000E-U6		固定接口：4GE 电+4GECombo+8GE 光 支持万兆接口 标配双电源(AC/DC 可选) 扩展槽：2*MIC+5*FIC 吞吐量：20Gbps

防火墙系列产品的特点是：

- 万兆多核全新硬件平台，打造业务永续的网络
  - 性能优异，实现海量业务处理

    15G 防火墙吞吐；200K 每秒新建连接数；400 万并发连接数；15K 并发 VPN 隧道；大容量 NAT 转换能力；轻松实现海量业务处理。
  - 高密度万兆接口，适应不同应用场景需求

    64 千兆+14 万兆的高密度接口，为提前跨入万兆时代的您提供不同组网情况下的安全防护，方便您细化安全区域。
  - 超长无故障运行时间，确保客户业务连续性

    关键部件冗余配置，成熟的链路转换机制，支持光、电两类内置 Bypass 插卡，为您提供超长无故障硬件保障；商用 10 年以上的超稳定软件平台，全球在线设备超过 10 万台，为您打造永续的办公环境。
- 超千种应用程序的精细管理，创建更高效的网络

- 广泛应用识别，实现网络可视化：150 名应用识别专家，超过 850 种可识别应用分类，让您一目了然网络带宽应用。
- 海量网站分类，营造绿色上网环境：6500 万海量网站，超过 130 种内容分类，屏蔽挂马、钓鱼等恶意网站，防范员工不当操作危害内网安全；隔离赌博色情等不良网站，营造绿色上网环境。
- 精细应用管理，创建高效办公网络：基于时间、应用、用户、带宽、连接数的多方位调控手段，可有效保障关键业务带宽，提升带宽利用率和员工工作效率，让 P2P/IM/Web 网站随您掌控。

- 专业内容安全防御技术的重新演绎，提供更安全的网络
  - 业界领先反病毒引擎，提供 99%高精准检出率：基于 Symantec 多年积累的反病毒技术，采用文件级内容扫描的 AV 引擎，结合全球领先的仿真环境虚拟执行技术，提供高达 99%的精准检出率，多次荣膺国际评测组织好评。
  - 专业漏洞补丁技术，让“变形”无所遁形：传统基于攻击代码的防护方式，因为攻击种类的频繁变形，需要维护更新庞大签名库，使得 IPS 引擎不堪重负，检测性能低下，误报漏报率较高。E1000E-X 采用 Symantec 领先的漏洞防护技术，针对漏洞（而非攻击代码）提供“虚拟补丁”，让各种攻击变形无所遁形。
  - 专业团队实时更新，实现零日攻击防护：全球部署的蜜网系统和超过 300 人的专业安全分析团队，持续追踪最新、最热门、最高危的系统漏洞和软件漏洞，以最快速的应对方案实现零日攻击防护，为您提供更安全的办公网络。
- 一键式配置，让策略调优化繁为简
  - 图形化配置界面，从此告别命令行：基于 Web 界面配置管理，更直观、更简单，彻底摆脱繁琐的配置。
  - 专业配置向导，轻松搞定策略配置：每项独立业务，均提供专业配置向导，让管理员轻松搞定策略配置。
  - 一键开启 IPS 和 AV，减轻维护工作量：基于 99%高精准检出率的 IPS/AV 规则库，无需调测，直接开启，将管理员从费时、费力、繁复的策略调优中彻底解放出来，真正实现快速部署，即插即用。

5.5 WLAN 产品

5.5.1 概述

WLAN 系列产品主要包括 AC6605 盒式 AC 和 S9700/7700 ACU 插卡式 AC，以及 AP6010SN/DN， AP6310SN， AP6510DN，AP6610DN 等多款 AP。

5.5.2 产品型号

表5-10 WLAN 产品

产品型号	设备外观图	备注
AP6010SN		室内型单频 AP
AP6010DN		室内型双频 AP
AP6310SN		经济型室分单频 AP
AP6510DN		标准型室外双频 AP
AP6610DN		全规格室外双频 AP
AC6605		盒式 AC
S9700/S7700 ACU 插卡		插卡式 AC

5.5.3 产品特点

AP6010SN

- 2x2 多入多出(MIMO)，2 条空间流
- 支持最大比合并(MRC)
- 支持 802.11n 和 802.11b/g 波束赋形
- 支持 20- 和 40-MHz 信道，PHY 数据速率高达 300Mbps
- 数据包聚合：A-MPDU(Tx/Rx)； A-MSDU(Rx only)
- 802.11 动态频率选择(DFS)

AP6010DN

- 2x2 多入多出(MIMO)，2 条空间流
- 支持最大比合并(MRC)

- 支持 802.11n 和 802.11a/g 波束赋形
- 支持 20- 和 40-MHz 信道，PHY 数据速率高达 300Mbps
- 数据包聚合：A-MPDU(Tx/Rx)；A-MSDU(Rx only)
- 802.11 动态频率选择(DFS)

AP6310SN

- 20- 和 40-MHz 信道
- PHY 数据速率高达 150Mbps
- 数据包聚合：A-MPDU(Tx/Rx)；A-MSDU(Rx only)
- 802.11 动态频率选择(DFS)

AP6510DN

- 2x2 多入多出(MIMO)，2 条空间流
- 支持最大比合并(MRC)
- 支持 802.11n 和 802.11a/g 波束赋形
- 支持 20- 和 40-MHz 信道，PHY 数据速率高达 300Mbps
- 数据包聚合：A-MPDU(Tx/Rx)；A-MSDU(Rx only)
- 802.11 动态频率选择(DFS)

AP6610DN

- 2x2 多入多出(MIMO)，2 条空间流
- 支持最大比合并(MRC)
- 支持 802.11n 和 802.11a/g 波束赋形
- 支持 20- 和 40-MHz 信道，PHY 数据速率高达 300Mbps
- 数据包聚合：A-MPDU(Tx/Rx)；A-MSDU(Rx only)
- 802.11 动态频率选择(DFS)

AC6605

- 高性能
  - 支持快速漫游（缓存 PMK）
  - 高达 512 APs 管理能力
- 高可靠
  - AC 设备间 1+1 双链路备份
  - 上行链路 LACP、MSTP 50ms 保护
  - 双电源接口，备份保护

- 风扇、电源热插拔，高温告警保护

- 强大的组网和业务能力
  - 丰富接口：2 个 10GE 光接口，4 个 GE Combo 接口，24 个 GE 电口。
  - 业务强大：精细化 QoS、丰富 L2/L3 功能、标准 MIB 接口。
- 保护投资
  - 无缝适应 WLAN 11b/g 和 11n
  - 华为标准软件平台，和宽带城域设备无缝融合

S9700/S7700 ACU 插卡

- AP 管理与用户接入
  - 大容量：每块 ACU 插卡支持管理 1024 个 AP，最大可支持管理 11K 个 AP
  - 支持按模板批量配置 AP
  - 灵活多样的用户认证模式：MAC、Portal 和 802.1x、Portal 免认证
  - 支持全局调优、局部调优和射频捕盲
- 安全及权限控制
  - 丰富灵活的用户权限控制，支持用户分组、隔离、ACL 等。
  - 支持多种安全协议标准：WEP、WPA/WPA2(PSK/1X)、WAPI
  - 支持密钥管理，支持 AP 黑名单
  - 防 STA IP 地址仿冒、ARP 攻击（DAI）、DHCP 服务器仿冒
- 无线网络
  - 支持 CAPWAP 隧道协议、线速转发
  - 支持 WMM、优先级映射、CAR、流级别定义，支持负载分担和 AC 备份
  - 灵活的组网模式（本地转发/集中转发/集中认证、本地转发，二三层组网）、WDS 网络部署