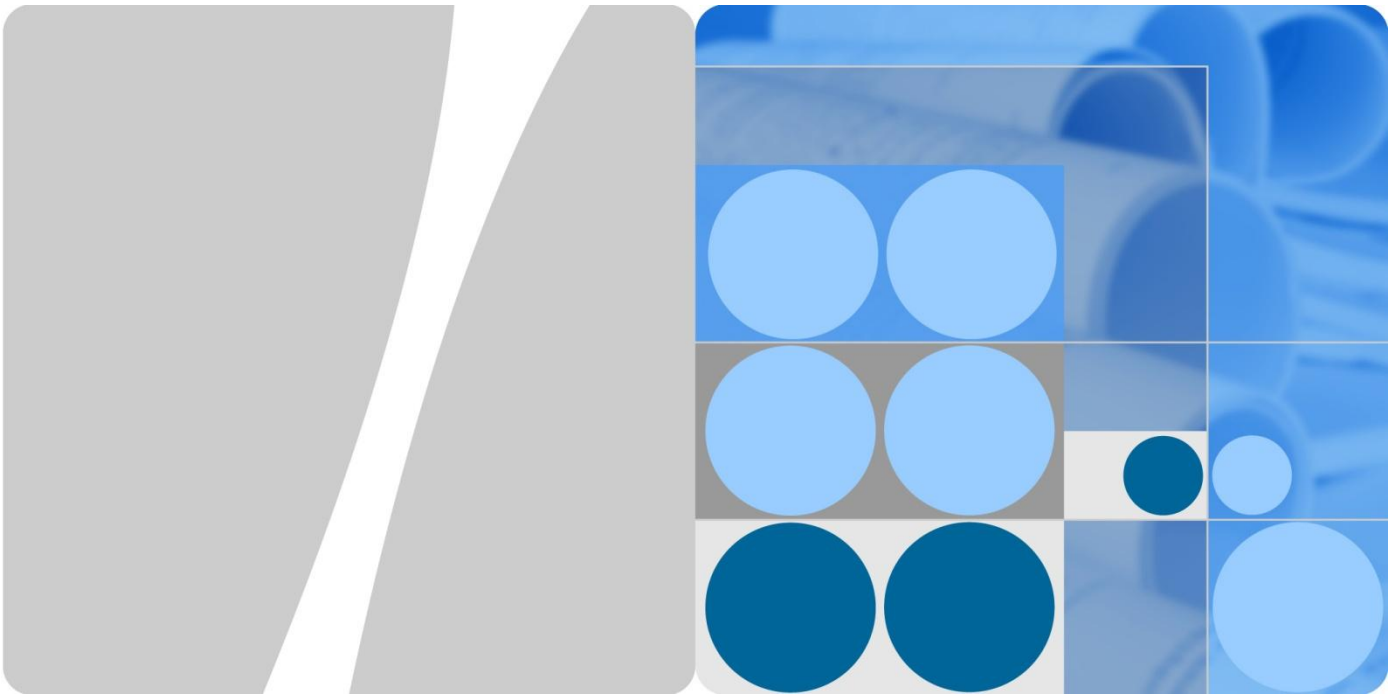
Doc. Code



华为融易分支网络解决方案
技术建议书

Issue 01

Date 2012-09-08

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

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默示的声明或保证。

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://www.huawei.com

Email: support@huawei.com

目录

1 分支网络概述.....4
1.1 分支网络概述.....4
1.1.1 分支网络概述.....4
1.1.2 分支网络的定义.....4
1.1.3 分支网络的需求.....5
1.2 分支网络设计原则.....5
1.3 华为分支网络的解决方案.....6
2 分支网络总体设计方案.....7
2.1 分支网络总体架构.....7
2.1.1 分支网络设计原则.....7
2.2 分支网络内部互联.....9
2.2.1 网络架构.....9
2.2.2 二层设计.....9
2.2.3 三层设计.....10
2.2.4 分支出口设计.....11
2.2.5 可靠性.....12
2.3 分支与总部互联.....14
2.3.1 互联技术介绍.....14
2.3.2 互联场景总述.....17
2.3.3 企业专线接入.....18
2.3.4 MPLS 网络接入.....19
2.3.5 因特网接入.....22
2.3.6 分支与总部互联技术比较.....28
2.4 分支安全.....29
2.4.1 分支安全挑战.....29
2.4.2 内网安全规划.....30
2.4.3 集成防火墙外网安全规划.....34
2.4.4 专业防火墙外网安全规划.....36
2.4.5 AR 集成防火墙部署规划.....42
2.4.6 专业防火墙部署规划.....44

2.4.7 NAC 解决方案 47
3 分支网络业务设计 59
3.1 Internet 访问 59
3.1.1 分支单链路接入 Internet 59
3.1.2 分支通过总部接入 Internet 60
3.2 语音 61
3.2.1 企业语音通信业务面临的挑战 61
3.2.2 企业语音通信业务的挑战目标 61
3.2.3 IP 语音系统设计的基本原则 62
3.2.4 语音基础知识 63
3.2.5 分支语音方案 67
3.3 Wlan 90
3.3.1 技术背景 90
3.3.2 WLAN 基本概念 90
3.3.3 WLAN 网络规划 97
3.3.4 WLAN 在分支网络中的应用 103
3.4 运维 108
3.4.1 分支运维发展面临的挑战 108
3.4.2 分支网络管理的融智方案 108
3.4.3 融智 eSight 在分支网络中的应用 110
4 分支网络场景设计 120
4.1 微型分支场景 120
4.1.1 对应的细分市场 120
4.1.2 网络设计要点 121
4.1.3 方案设计 122
4.1.4 典型配置建议（推荐产品、板卡） 134
4.2 小型分支场景 136
4.2.1 对应的细分市场 136
4.2.2 网络设计要点 137
4.2.3 方案设计 137
4.2.4 典型配置建议（推荐产品、板卡） 150
4.3 中型分支场景 152
4.3.1 对应的细分市场 152
4.3.2 网络设计要点 152
4.3.3 方案设计 153

1 分支网络概述

1.1 分支网络概述

1.1.1 分支网络概述

经济全球化发展，企业规模逐步扩大，分散在不同地理位置的分支机构大量出现，企业人员，特别是非专业人士，如何支撑海量分支网络，实现业务正常流转？Gartner 预计，到 2015 年大多数企业的 IT 支出中有 35%将在 IT 部门的预算之外。另外，竞争加剧市场多变，企业需要通过分支的快速搭建和灵活迁移来适应多变的市场，满足客户本地化、定制化需求，实现业务驱动？企业业务模式的改变，要求企业搭建部署更简单、运维更轻松的分支网络。

同时，员工的工作方式也在悄悄发生变化。首先，业务更加复杂，需要不同地域的员工、合作伙伴等充分发挥各自优势，深度合作，才能快速高效完成。而视频会议、电话、邮件等以其便捷、低成本成为企业和员工的远程沟通的优选，在企业中迅速普及。其次，员工活动范围更广，移动性比任何时候都强，移动办公、BYOD、应急通信等成为趋势，企业网络需要随时随地的接入。受限于 IT 投资成本，企业要求搭建多元承载的网络。网络覆盖更广、移动性更强，使企业网络面临更多的威胁。所有这些都要求分支网络更安全。

华为公司深度剖析企业对分支网络的需求，提出融易分支解决方案：融合分支，多元承载安全护航,；简易分支，部署简单运维轻松。

1.1.2 分支网络的定义

分支网络一般是指企业或者大型机构网络的延伸，通过广域网互联的方式与企业总部相联。分支网络的主要目的是使企业业务能够得到更好的扩展与延伸。

目前我们通常涉及的分支网络包括微型分支、小型分支、中型分支和大型分支。主要根据固定接入点数量来划分分支规模：

- 微型分支（接入点数<10）主要应用场景包括微型金融机构，离行 ATM 机，移动柜台，环境检测车
- 小型分支（接入点数 10-50）主要应用场景包括银行/证券/税务营业网点，小型企业分支，连锁超市
- 中型分支（接入点数 50-250）主要应用场景包括大型银行/证券营业网点、分行/支行，中小酒店，中小医疗机构
- 大型分支（接入点数>250）主要应用场景包括大型企业分支机构，大型酒店，大型医疗机构

1.1.3 分支网络的需求

随着用户对 IT 成本、效率和体验的更高要求，让分支网络面临了更大挑战，分支网络变得更加复杂。如何使分支网络能够更好的为企业服务，如何解决协同工作，如何解决运维等对我们的分支网络建设提出了新的需求。

- 需要多业务融合

  分支机构数量越来越多较多，业务融合需求强，来节省单个分支网络投资
- 需要移动承载

  移动终端越来越多，移动应用越来越多，业务逐渐向移动承载迁移
- 保证高安全

  分支与总部间的流量属于内部业务，分支与总部往往通过公网连接
- 需要灵活互联

  分支机构需要各种业务接口方式提供互联，包括：有线接入，3G/LTE 无线接入，专线接入，拨号接入，电口接入，光口接入等
- 容易部署

  无需建设专门机房，提供快速开展业务
- 易运维

  分支机构数量多，分支机构不配备专门 IT 人员，难以维护

1.2 分支网络设计原则

企业分支网络是企业拓展业务必须建设的信息平台，应本着以下原则进行建设：

- 可靠性，可用性

  分支网络一般不会部署完整的 IT 应用系统。因此，在日常办公中需要通过访问总部网络的相关资源，才能正常开展工作。一旦分支和总部的网络连接中断，很多正常业务都将无法开展，为此分支网络的可靠性和可用性要求很高。
- 可扩展性

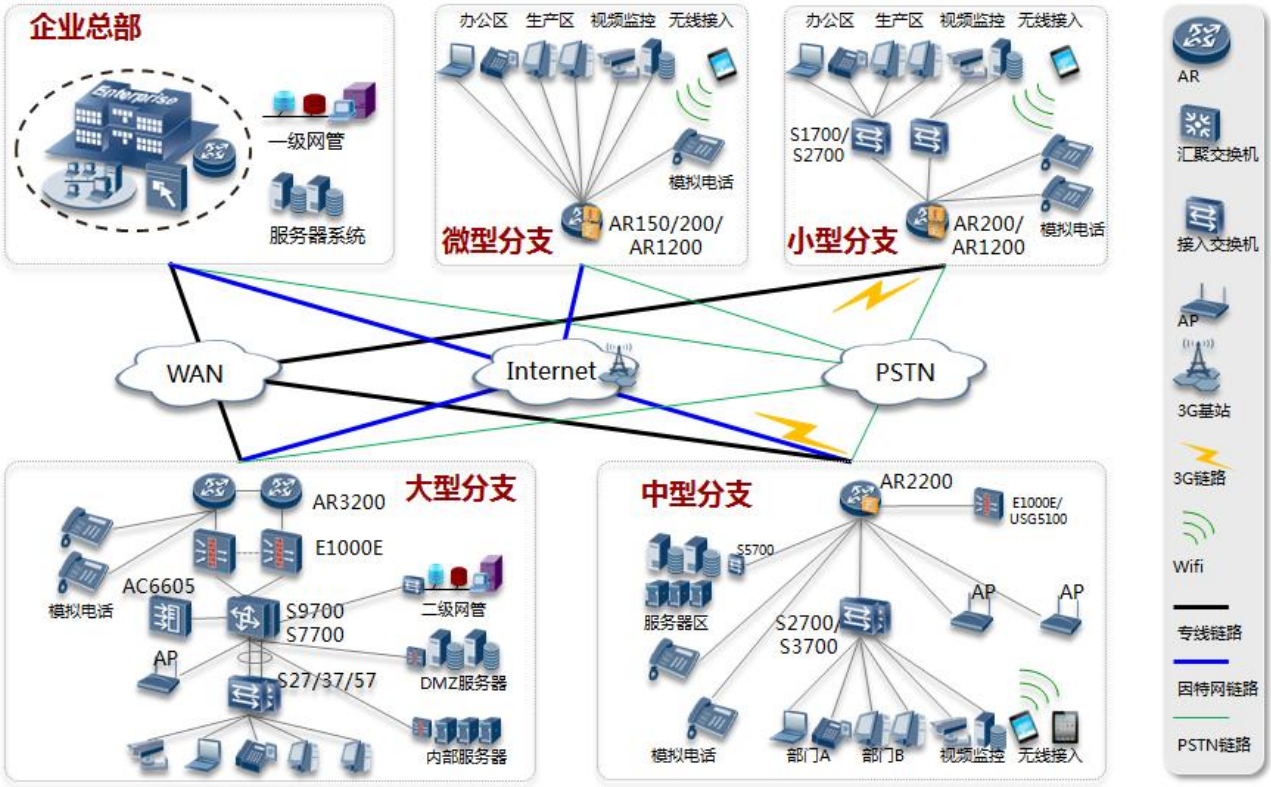
  分支网络的建设需要充分考虑后续分支机构规模扩大的可能性。基于此，推荐采用分层的网络设计；每个层次的设计采用模块化的可扩展设计。
- 安全性

  由于分支网络需要经常性和总部进行互联，为此，分支网络的安全性必须要做到和总部网络类似，否则容易导致分支网络成为黑客进入总部网络的一个跳板。
- 经济性

  随着企业的业务发展，分支数量可能会持续增加。为了降低企业的运营成本，在分支网络的建设中，必须考虑尽量降低每个分支网络的建设成本。

1.3 华为分支网络的解决方案

华为公司提出 ONE NET 解决方案，是基于标准化、协同、一揽子的分支网络解决方案。



融易分支全景图

2 分支网络总体设计方案

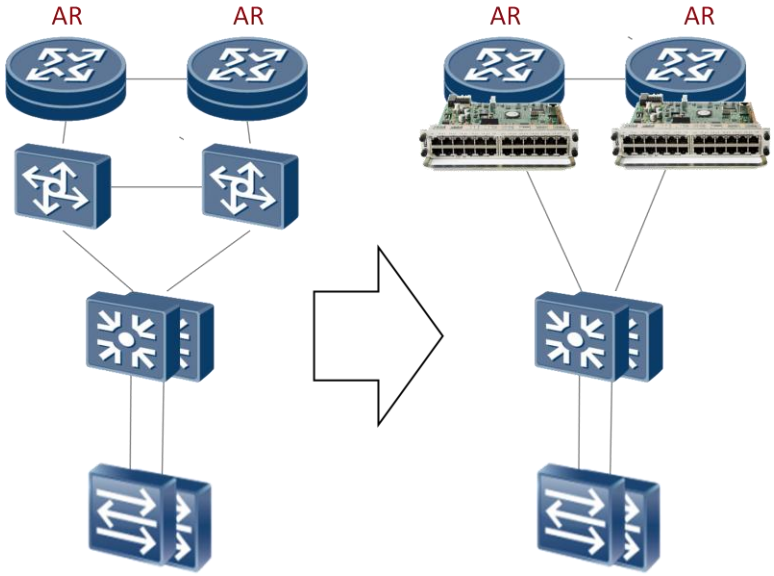
2.1 分支网络总体架构

2.1.1 分支网络设计原则

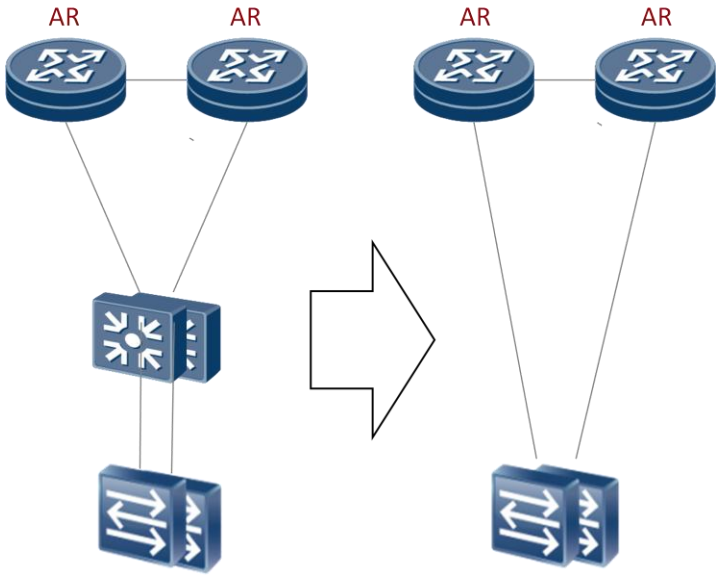
根据企业分支规模选择不同的组网模型，保障企业业务运行的同时节省企业建网成本，应本着以下原则进行建设：

- 简洁化设计

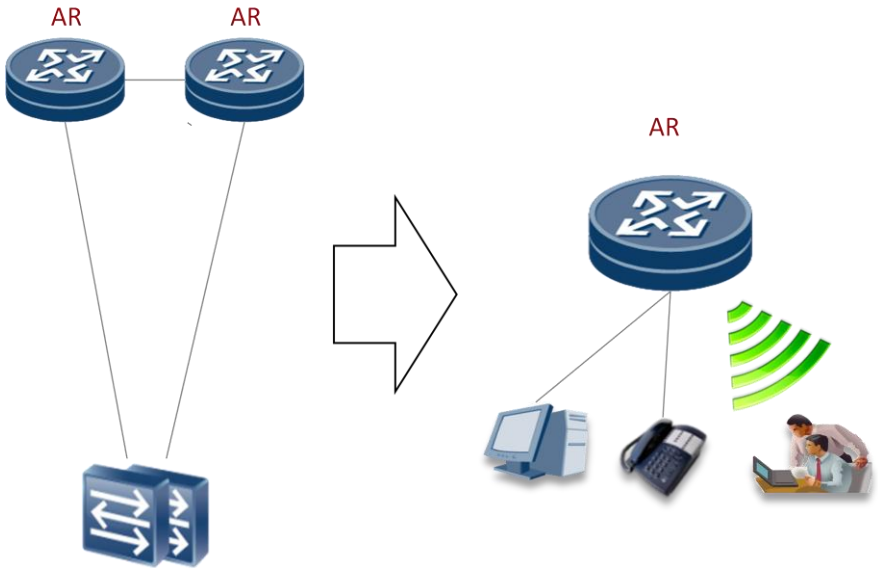
大型分支：业务流量主要以纵向流量为主（总部<->分支），横向流量不大（分支内流量），可以使用 AR 高端接入路由器兼做核心层功能，将原先的四层网络架构优化至三层，在满足大型分支业务的前提下，降低建网成本，减少网络维护工作量。AR 提供 24*GE 高密度板卡，通过多链路捆绑技术解决大流量的三层转发。



中型分支：业务流量主要以纵向流量为主（总部<->分支），横向流量少（分支内流量），并且中型分支网络设备数少，可以使用 AR 高端接入路由器兼做汇聚层功能，将原先的三层网络架构优化至两层，在满足中型分支业务的前提下，降低建网成本，减少网络维护工作量。AR 提供 8FE/1GE 板卡，通过多链路捆绑技术解决大流量的三层转发。



小、微型分支：业务流量主要以纵向流量为主（总部<->分支），横向流量很少（分支内流量），并且小、微型分支网络设备和接入点数量少，可以使用 AR 高端接入路由器将原先的二层网络架构优化至一层，通过 AR 高端接入路由器实现全业务接入，在满足小、微型分支业务的前提下，降低建网成本，减少网络维护工作量。



- 集约化设计

随着分支业务需求的多样化（数据、语音、视频），业务接入的多样化（有线、无线）和安全需求的多样化（VPN、防火墙），如何使用少量设备实现众多业务需求，简化运维管理，降低企业投入成本是对分支网络设计的迫切要求。AR 高端接入路由器采用集约化设计，实现多业务融合，并且提供卓越的转发性能，成功解决客户对分支关键设备的诉求。

1、 AR 集成 IP 语音的处理能力，支持 SIP-AG 和 PBX 功能，满足语音应用场景的需求。

2、 AR 集成 AC 功能，只需要在覆盖区内布放 AP 设备，即可与 AR 实现分支 WLAN 覆盖，无需独立 AC 设备，简化网络结构，方便运维。

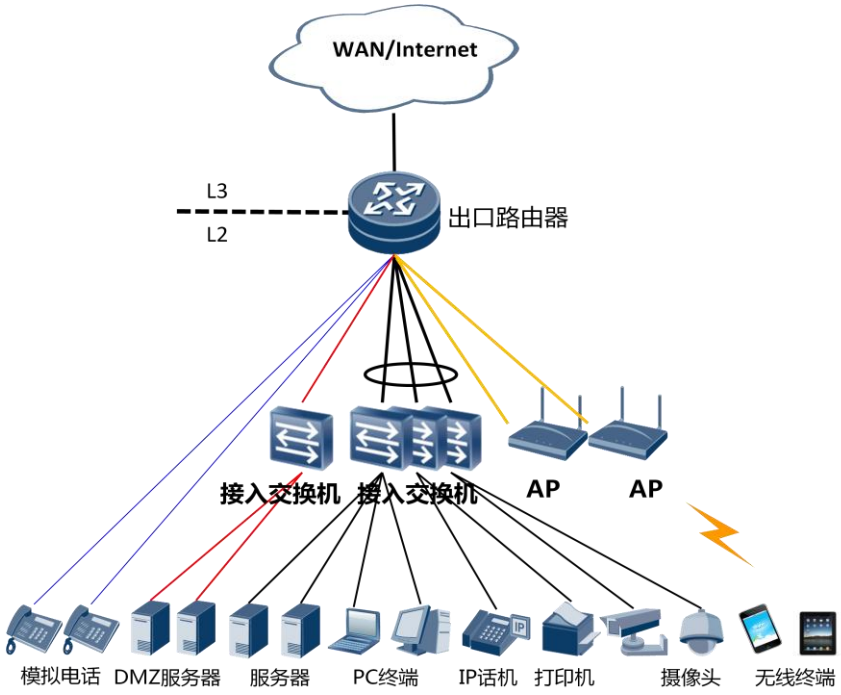
3、 AR 集成 VPN 功能，无需另行部署 VPN 设备即可实现 IPSEC VPN/SSL VPN 接入，减少客户投入。并且 AR 采用 IPSEC 硬件加速引擎，不影响三层转发业务。

4、 AR 集成防火墙功能，可以满足大部分分支对安全的需求，包括安全域隔离、状态防火墙、防攻击等等。

2.2 分支网络内部互联

2.2.1 网络架构

企业分支采用出口路由器作为二三层分界点，分支内部基于二层转发，分支出口部署路由协议与 WAN/Internet 实现互通。出口路由器部署 NAT 功能，实现与 Internet 互访。

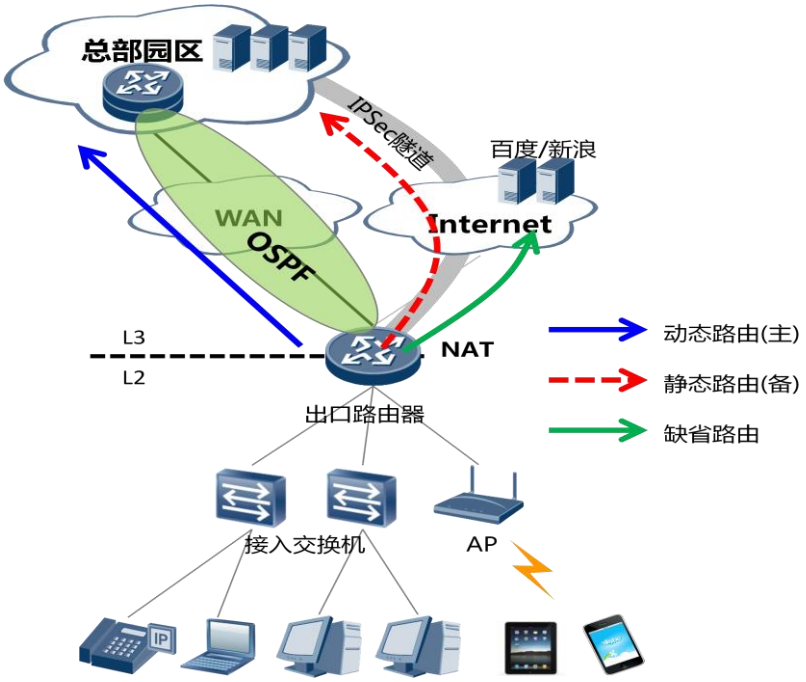


2.2.2 二层设计

- 终端接入：有线用户连接到接入交换机，同一交换机使用相同 VLAN，不同交换机使用不同 VLAN，出口路由器作为有线用户网关。出口路由器支持 AC 功能，管理下联 AP，AP 为无线用户提供 WLAN 接入，出口路由器作为无线用户网关。模拟话机连接到路由器语音板，出口路由器根据业务部署可以作为 PBX 或 SIP AG 实现语音通信。
- 接入设计：出口路由器支持防火墙功能，基于不同端口划分安全域，使不同安全域的交换机连接到出口路由器不同端口，通过出口路由器进行安全控制。同一安全域的接入交换机使用堆叠技术，将多台交换机虚拟为一台设备，简化管理，提升设备

可靠性。虚拟化后的交换机通过链路捆绑上行，增加上行带宽的同时提供了链路可靠性。

2.2.3 三层设计

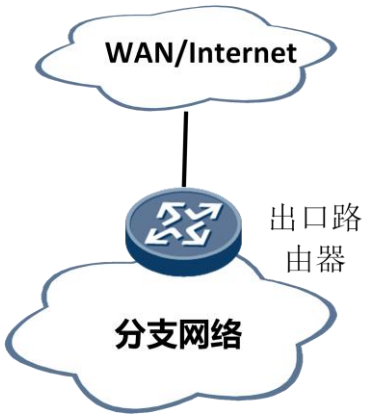


出口路由器有 WAN 和 Internet 出口，通过动态路由、静态路由或缺省路由实现与总部和 Internet 网络的互联。

- 动态路由：出口路由器通过 WAN 口与总部路由器之间运行动态路由协议（OSPF、RIPv2 等），分支和总部互相学习到精确路由，分支内流量基于学习到的路由表进行三层转发。
- 静态路由：分支在基于 Internet 链路的 IPSec 隧道上配置到总部的静态路由，其优先级低于动态路由，作为 WAN 链路的备份路由。因为流量需要穿越 Internet，IPsec 封装方式建议采用隧道模式和 ESP 加密传输，以确保分支数据在公网传输的安全性。当动态路由失效后，分支内流量通过 IPSEC 方式实现与总部互访。建议 WAN 链路配置 BFD 实现链路故障检测，以降低 WAN 链路故障时流量切换的时延。
- 缺省路由：出口路由器部署 NAT 功能，视具体的接入方式，在 Internet 接口链路上自动生成或者手动配置缺省路由，为用户上网流量提供路由。

2.2.4 分支出口设计

单链路上行



企业分支单链路上行 WAN 或 Internet，适合对可靠性要求不高的微/小型分支。如果分支通过 WAN 上行，分支直接通过 WAN 网络访问总部，分支访问 Internet 的流量需要通过总部进行转发。如果分支通过 Internet 上行，分支直接访问 Internet，分支访问总部的流量需要通过 IPSEC 方式加密传输到总部。

双 WAN 上行

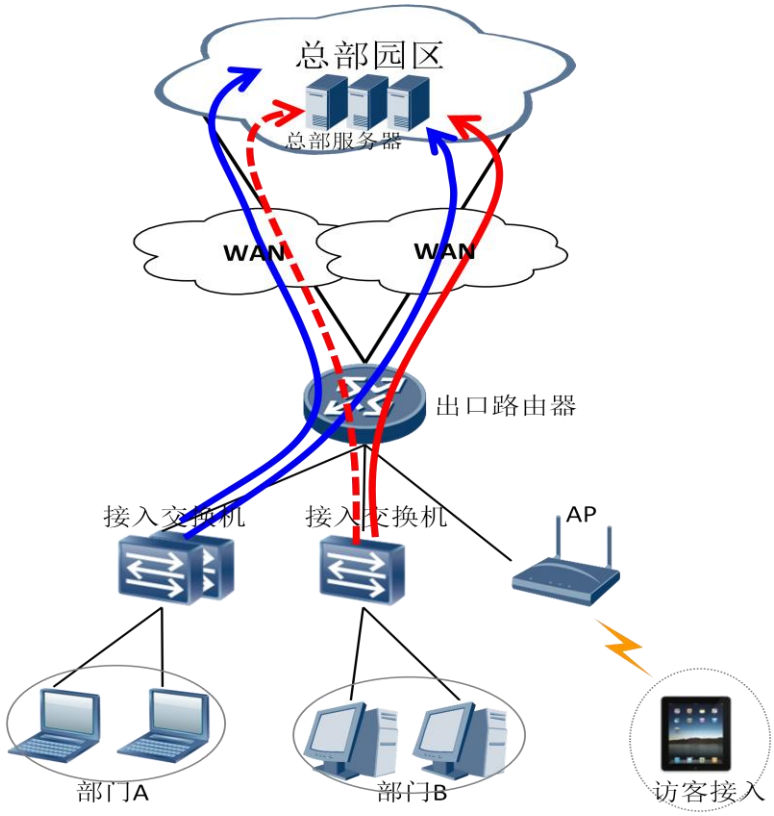
企业分支双 WAN 上行，适合对安全性/可靠性要求极高的场景，如银行网点。建议出口路由器 WAN 链路间采用负载分担模式，实现流量的负载均衡，并且当单链路故障时，需要确保所有流量转发不丢包，建议负载分担模式下单链路带宽利用率控制在 50%以下。分支访问 Internet 的流量需要通过总部进行转发，总部可以进行统一安全管理，确保分支访问 Internet 的安全性。

WAN+Internet 上行

企业分支采用 WAN+Internet 上行，适合上网流量大且本地部署安全措施的场景。分支访问总部的流量通过 WAN 链路转发，并且分支与总部建立 IPSec 隧道，以确保 WAN 链路故障时分支与总部的互访。分支访问 Internet 的流量通过出口路由器做 NAT 穿越，无需绕行到总部。

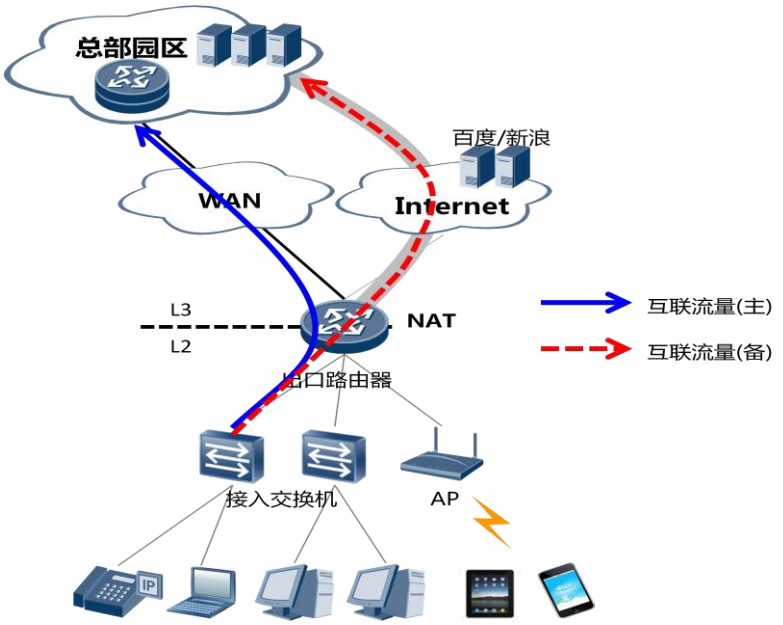
2.2.5 可靠性

出口可靠性（负载分担）



- 基于动态路由：出口路由器通过两个 WAN 网络与总部网络间运行动态路由协议，出分支流量根据路由选择出口链路，也可以根据业务优先等级针对不同部门业务选择不同的出口链路，实现业务流向的可控管理。
- 基于静态路由：出口路由器配置静态路由，指定到总部的某些访问走指定出接口，可以很好的规划分支访问总部的流量路径，需要部署 BFD 机制与静态路由联动，以避免链路单通等故障引起的业务转发不通。
- 基于源地址路由：出口路由器执行源地址路由，按照网段将业务分配到不同 WAN 链路，实现业务隔离。两条 WAN 链路分别配置 BFD 检测，任一链路出现故障后，源地址路由策略失效，业务切换到另一条 WAN 链路。源地址路由要求总部出口路由器配置静态路由，保证回程选路的一致性。

出口可靠性（主备链路）



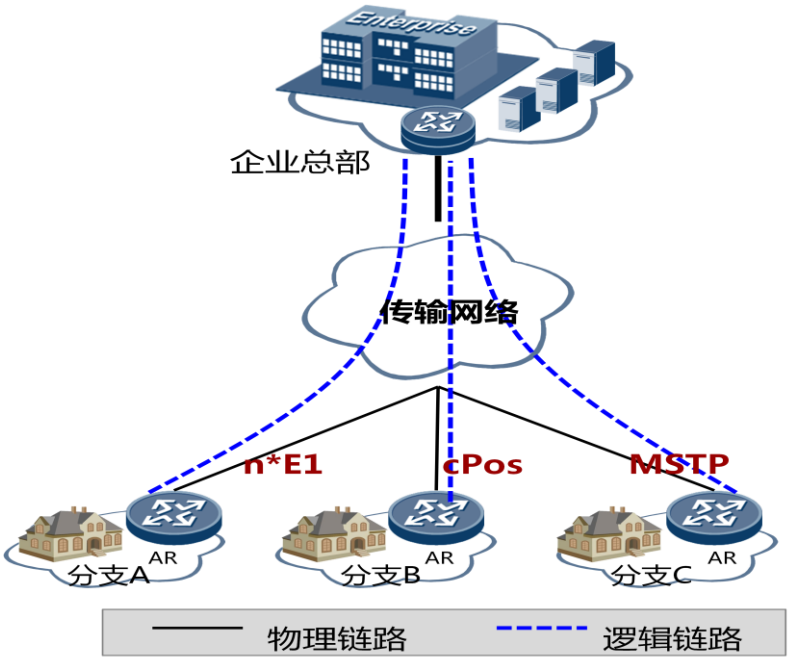
- 主用链路：分支通过 WAN 链路与总部路由器运行动态路由协议，互相学习到精确路由。分支与总部互访流量通过 WAN 转发。
- 备用链路：Internet 上建立的 IPSec 隧道做为 WAN 链路的备份，建议采用隧道模式和 ESP 加密传输，以确保数据在公网传输的安全性。出口路由器配置到总部的静态路由，并保证路由优先级低于动态路由。
- 主备链路切换：WAN 链路质量优于 Internet 链路，WAN 链路配置 BFD 检测，快速检测链路状态，以降低 WAN 链路切换的时延。WAN 链路正常时，分支访问总部数据按照动态路由转发；当 WAN 链路故障后，BFD 触发动态路由收敛，流量切换到 IPSec 隧道转发。当 WAN 链路故障恢复后，流量自动切换回 WAN 链路。

2.3 分支与总部互联

2.3.1 互联技术介绍

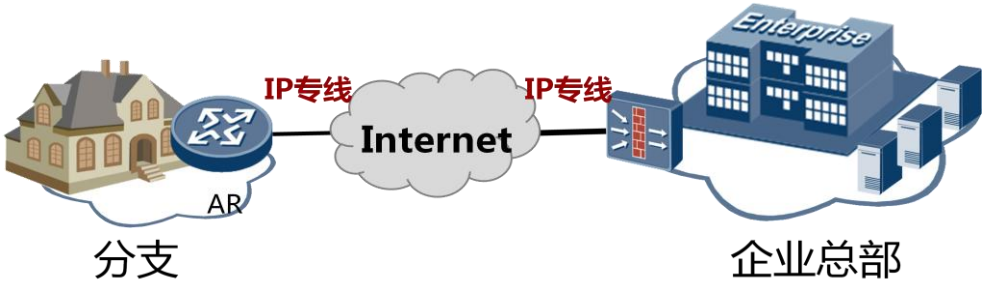
分支互联技术分为传输专线接入技术、IP 专线&拨号接入技术、3G 接入技术、XPON 接入技术等，基于分支出口的链路接入方式和分支对质量的不同要求，可以选择上述多样的接入技术实现分支与总部的访问。

传输专线接入

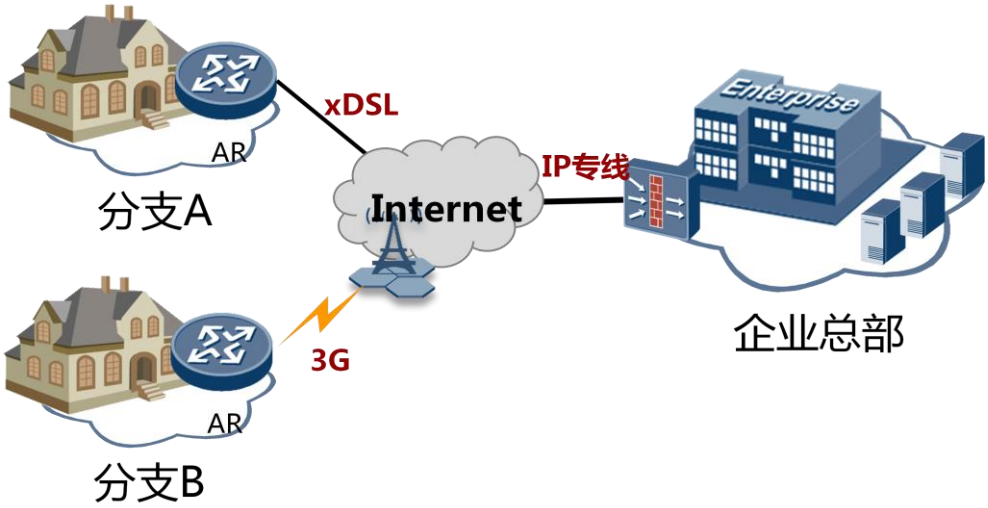


传输专线的特点是 E1/CPOS/MSTP 都是基于 SDH 的物理线路，可靠性和安全性很高，传输专线属于链路独占，链路带宽和 QoS 有保障。从物理上看是总部到多个分支的点到多点链路，实际从逻辑上看是点到点的连接。传输专线适用于广域互联和骨干网节点互联，以及对高可靠性、高安全性、QoS 保障有严格要求的场景。

IP 专线&拨号接入

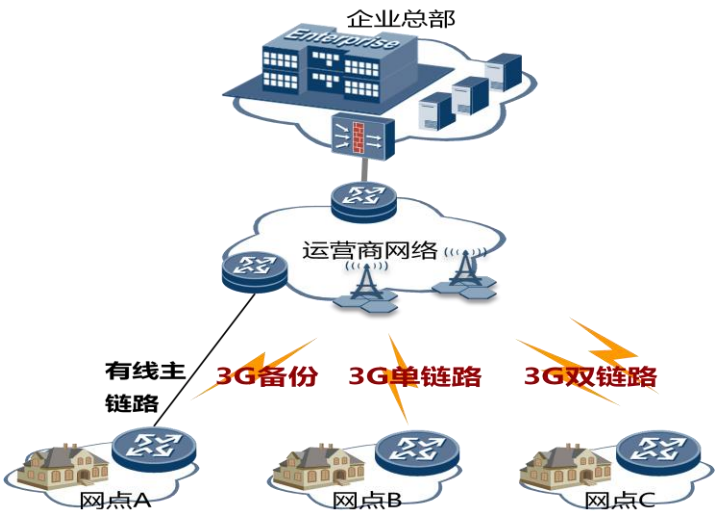


分支出口路由器 IP 专线地址由运营商统一分配，通常采用静态配置的方式。IP 专线带宽由运营商灵活配置，分支企业可以根据自身对带宽的需求向运营商进行申请。运营商对分支企业的业务进行 QoS 保障，能够有效保证分支业务的质量要求。IP 专线接入适用于大带宽接入、网络内部有供外部访问服务器和对 QoS 要求高的场景。



拨号接入特点是接入灵活，只要有电话线和 3G 接入场景就可以采用拨号接入方式。通过拨号接入 Internet 网络，价格低廉但上行接入带宽不高。拨号接入场景对 QoS 保障一般，尤其是 3G 场景，信号易受干扰，链路质量不高。分支出口路由器通过拨号获取公网地址，通过 IPSEC 隧道实现与总部的互通。如果分支需要分配总部的私网地址，则可以采用 L2TP 方式承载 PPP 会话报文到总部进行认证，并从总部获取 IP 私网地址，实现与总部的互访。

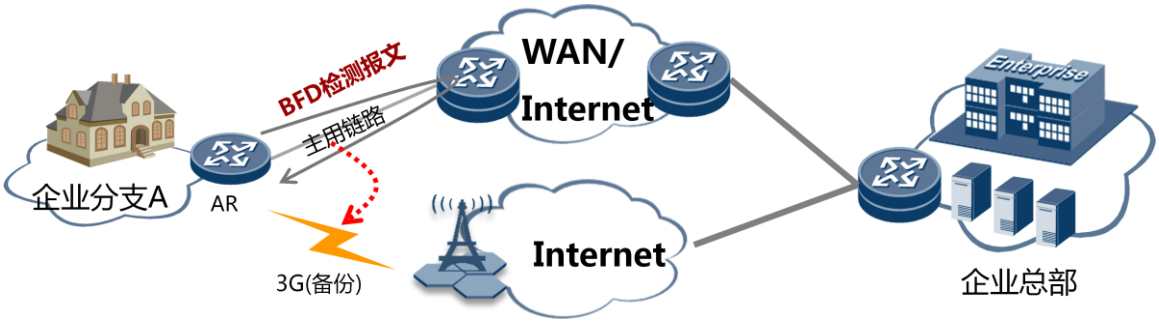
3G 接入



3G 接入场景分为 3G 备份场景、3G 单链路场景和 3G 双链路场景，根据客户上行链路状态选择 3G 的接入场景。

- 3G 备份场景是 3G 作为有线链路的备份链路，当有线链路正常时，3G 链路不拨号，不产生任何费用。当有线链路故障时，基于流量触发 3G 拨号，3G 链路获取地址后进行流量转发，此时 3G 链路为转发主链路。当有线链路故障恢复后，将流量从 3G 链路回切到有线链路，同时拆除 3G 链路。3G 备份场景采用按照流量计费方式，可以最大程度的节省企业开支。
- 3G 单链路场景适用于无有线链路并且对质量要求不高的场景，采用 3G 拨号方式获取地址可以通过 IPSEC 方式与总部互通，也可以在该端口做 NAT 功能，实现分支与 Internet 的互访，该场景建议采用包月计费方式，可以很好的节省企业开支。
- 3G 双链路场景适用无有线链路并且可靠性要求高，需要进行负载分担或主备链路场景。AR 部署策略路由，上行流量在两条 3G 链路分担，两条 3G 链路互为备份。负载分担模式下两条 3G 链路双活，费用较高。采用主备链路模式时可以选择主链路包月计费，备份链路按流量计费，可以很好的节省企业开支。

3G 备份链路可靠性



3G 做备份链路时，需要快速检测到有线链路故障实现 3G 链路拨号和流量切换，降低切换时延，需要部署 BFD 检测机制。

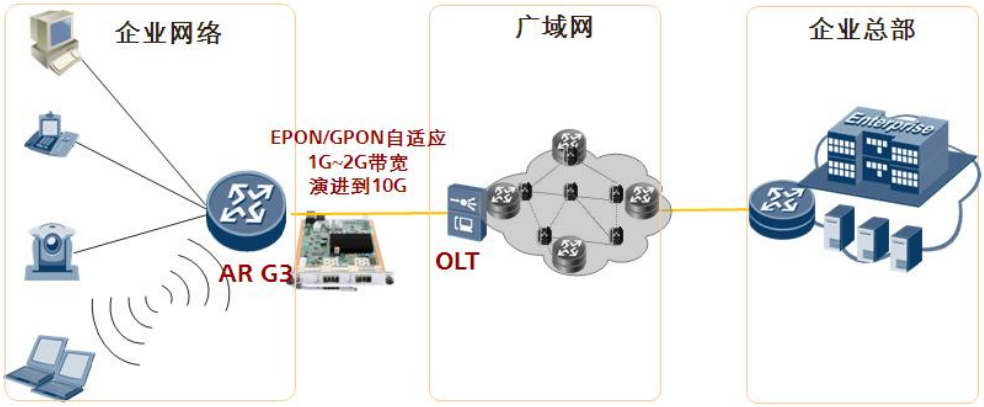
（1）AR 主链路部署单臂 BFD 检测机制，实时监测该链路的连通状况。

（2）建立 3G 备份链路跟踪主链路 BFD 会话的状态。

（3）主链路 BFD 会话 Down 后，触发 3G 拨号，3G 链路 up，路由收敛后，分支流量切换到 3G 链路。

（4）原先的主链路恢复后，路由切换，分支流量重新切换回有线链路，并拆除 3G 链路。

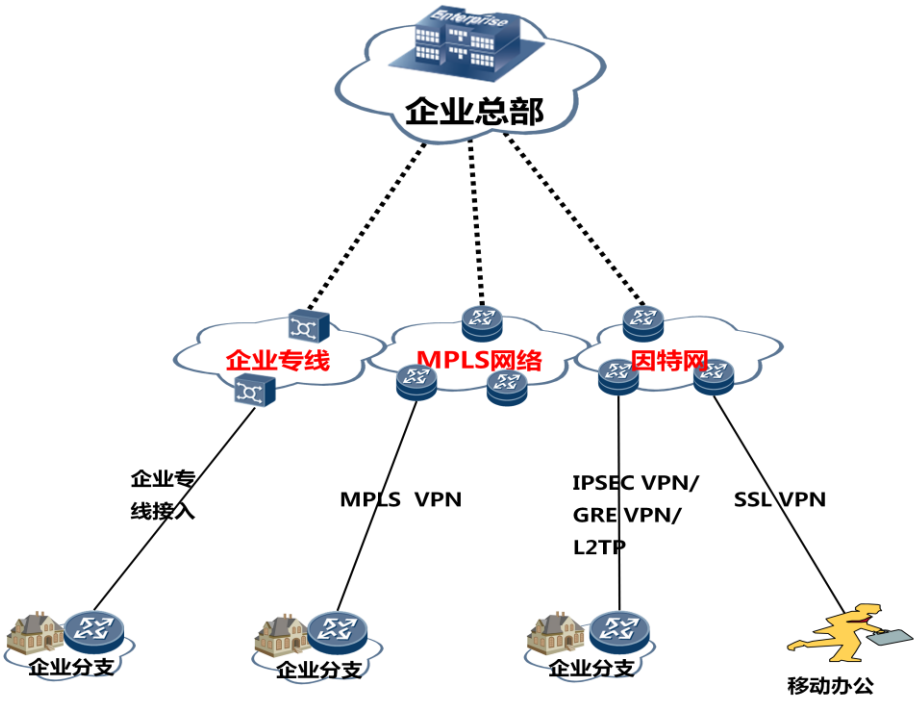
XPON 接入



目前运营商 FTTH 建设普及，光进铜退，PON 接入逐渐成为主流。PON 采用无源光纤传输技术，比传统专线可靠性高，覆盖距离广。PON 当前网络带宽是 1G，未来可以演进到 10G，网络带宽充裕。PON 接入适用于企事业单位 XPON 专线的上网场景，例如酒店、政府、医疗等，这些行业对上网的可靠性要求高，通常带宽要求在 8M~40M 之间，对上网费用不是很敏感。

2.3.2 互联场景总述

根据分支出口运营商链路类型及分支对网络质量要求，可以采用如下三种方式实现分支与总部互联：



企业专线

大集团、大型企业分支与总部互联，要求链路专用，对质量和安全有特别高的要求，企业专线的优点是专线专用、带宽独享，可充分保障数据传输的安全性、及时性。缺点是总体成本高、网络建设时间长，后期网络扩容、改造困难，无法满足移动办公需要。

MPLS 网络

没有广域专网、对网络质量有要求的大中型分支机构与总部互联。MPLS 网络的优点是运营商代维管理，业务开通时间短，质量和带宽有保障。缺点是对于企业出口路由器规格和性能要求高，专业技术要求高。

因特网

对网络质量无具体要求的微小型分支与总部互联。因特网的优点是接入方式灵活，随时随地与总部互通，费用低廉。缺点是无质量保障、无带宽保证。

2.3.3 企业专线接入

传统专线主要是指物理层专线，包括 SDH/SONET、E1/T1、E3/T3 和 MSTP 等，运营商仅提供一层连通性。这种专线带宽是预留、独占的，线路质量一般也比较好，其价格主要与带宽、距离以及连接的站点数量有关，相对其它专线而言价格较高。为此，传统专线一般仅用于将分支和总部连接，而且大都用于和总部在地理上距离较近的分支，并且分支存在对带宽、时延、抖动等有严格要求的应用，还有就是没有其它可选择的 WAN 连接方式。

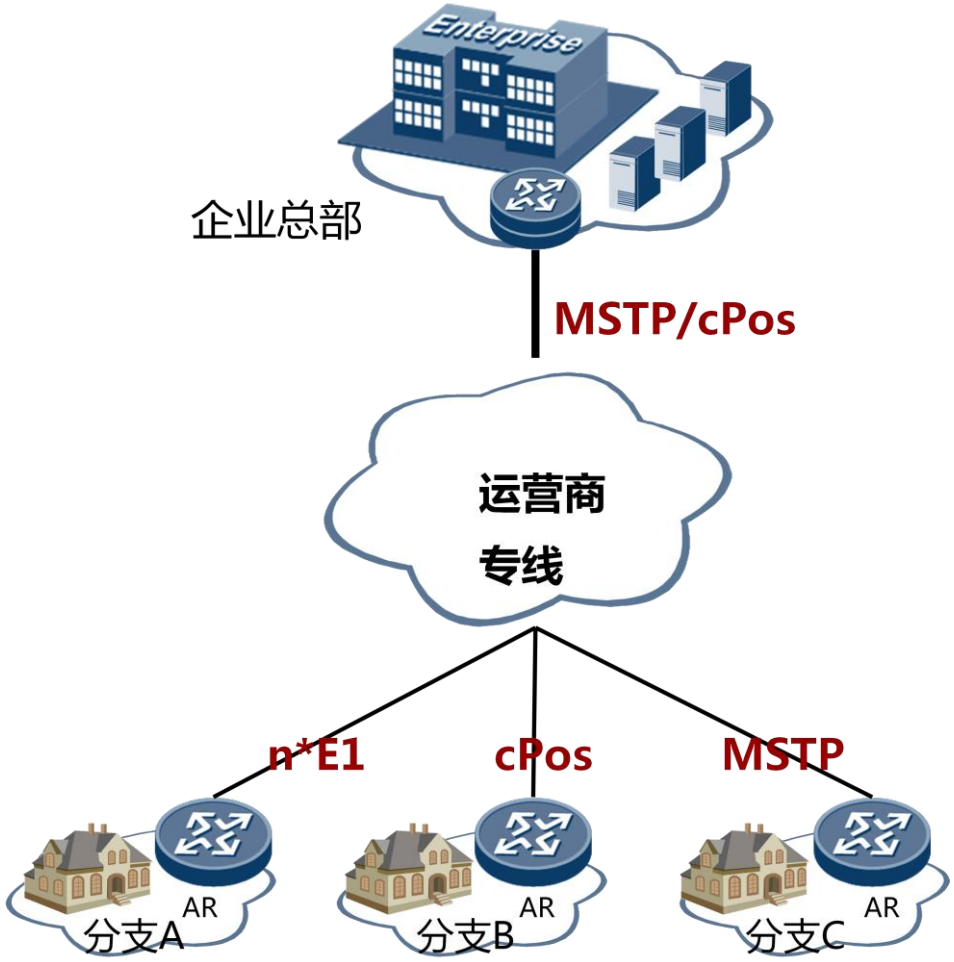
采用传统专线时，必须为所有穿越 WAN 的流量选择合适的链路层协议。WAN 链路协议的选择必须考虑正在使用的 WAN 技术和通信设备。当前最流行的链路层协议如下：

（1）PPP(Point-to-Point)：这是在点到点链路上传送 IP 报文的最流行的封装协议。它提供了同步和异步封装，网络协议复用、链路配置、链路质量测试、错误检测、可选的能力协商，如网络层地址和数据压缩算法等功能。

（2）MLPPP(Multilink Point-to-Point)：一种用于将数据报文在多条 PPP 链路上拆分、重组和排序的方法。它将多条物理链路组合成一条逻辑链路，增加了链路的带宽和可靠性，与以太端口的链路聚合类似。

（3）以太网：以太网可以提供 10M/100M/1000M/10GE 等多种速率的连接，并且还有很多不同的接口形式和传输介质，如网线和单模/多模光纤等。

采用此类专线，二层和三层网络完全由企业自己规划，为企业自己部署 MPLS VPN 等提供了很好的条件，但同时也要求企业具有比较强的技术能力。



2.3.4 MPLS 网络接入

企业专网的应用，促使了企业效益的日益增长，但传统专网（如 ATM 等）难以满足企业对网络的灵活性、安全性、经济性、扩展性等方面的要求。这促使了一种新的替代方案的产生——在现有 IP 网络上模拟传统专网；这种新的解决方案就是虚拟专用网 VPN（Virtual Private Network）。

- VPN 是依靠 Internet 服务提供商 ISP（Internet Service Provider）和网络服务提供商 NSP（Network Service Provider）在公共网络中建立的虚拟专用通信网络。VPN 具有以下两个基本特征：

1、 专用（Private）：对于 VPN 用户，使用 VPN 与使用传统专网没有区别。VPN 与底层承载网络之间保持资源独立，即 VPN 资源不被网络中非该 VPN 的用户所使用；且 VPN 能够提供足够的安全保证，确保 VPN 内部信息不受外部侵扰。

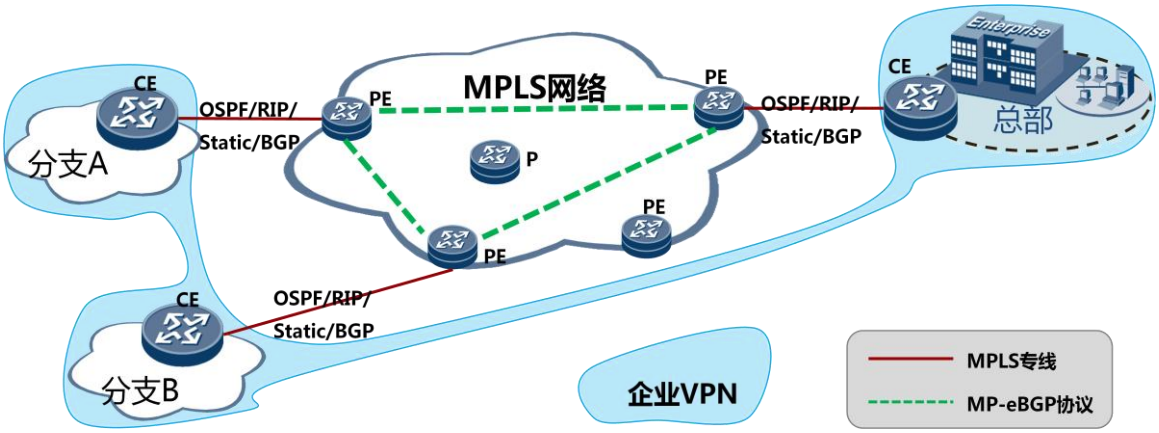
2、 虚拟（Virtual）：VPN 用户内部的通信是通过公共网络进行的，而这个公共网络同时也可以被其他非 VPN 用户使用，VPN 用户获得的只是一个逻辑意义上的专网。这个公共网络称为 VPN 骨干网（VPN Backbone）。

3、

MPLS VPN 主要分为 L3VPN 和 L2VPN。

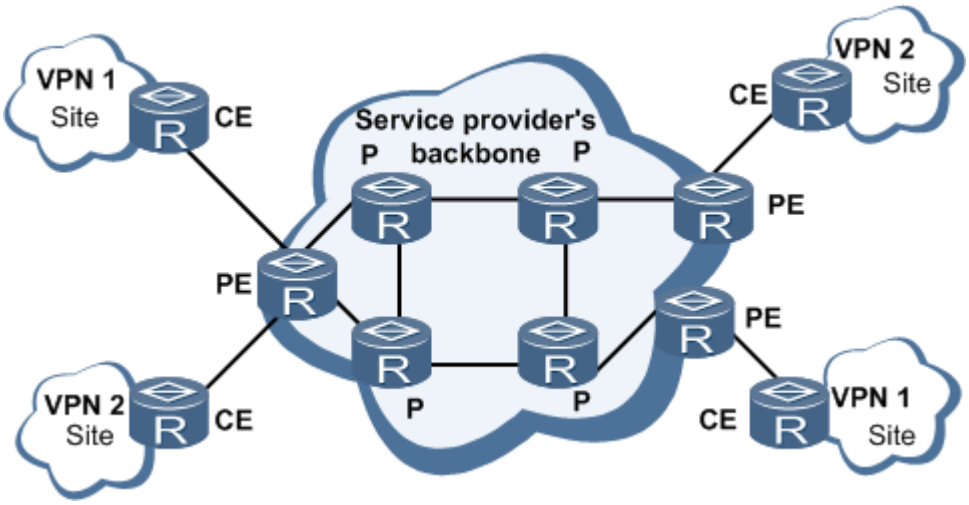
1、 三层 VPN，即 BGP/MPLS IP VPN，它使用 BGP（Border Gateway Protocol）在服务提供商骨干网上发布 VPN 路由，使用 MPLS（Multiprotocol Label Switch）在服务提供商骨干网上转发 VPN 报文。这里的 IP 是指 VPN 承载的是 IP 报文。BGP/MPLS IP VPN 的基本模型由三部分组成：CE、PE 和 P。三层虚拟专线控制平面复杂，技术要求较高，需要运营商协助私网路由的扩散，但发展最为成熟，在有关 VPN 跨越、可靠性和各种复杂场景都有较好的解决方案，适合大规模和复杂场景下的网络部署。

2、 二层 VPN，MPLS L2VPN 提供基于 MPLS 网络的二层 VPN 服务，使运营商可以在统一的 MPLS 网络上提供基于不同介质的二层 VPN，如 ATM、FR、VLAN、Ethernet 和 PPP。简单来说，MPLS L2VPN 就是在 MPLS 网络上透明传输用户二层数据。从用户的角度来看，MPLS 网络是一个二层交换网络，可以在不同节点间建立二层连接。主要包括 VLL 和 VPLS 两种方式。二层虚拟专线不涉及复杂的私网路由扩散等过程，技术相对简单，内部路由完全由自己控制。如果使用点到点专线，则要求有较多分支的企业需要租用大量的专线，费用会比较高；如果使用 VPLS，则在分支站点多的情况下，广播流量会比较多，并且不易控制分支之间的互通。总的来说，MPLS 的二层 VPN 适合分支节点不多的场景，如果分支节点较多，则不推荐使用。



BGP/MPLS IP VPN

BGP/MPLS IP VPN 是一种 L3VPN（Layer 3 Virtual Private Network）。它使用 BGP（Border Gateway Protocol）在服务提供商骨干网上发布 VPN 路由，使用 MPLS（Multiprotocol Label Switch）在服务提供商骨干网上转发 VPN 报文。这里的 IP 是指 VPN 承载的是 IP 报文。
BGP/MPLS IP VPN 模型：



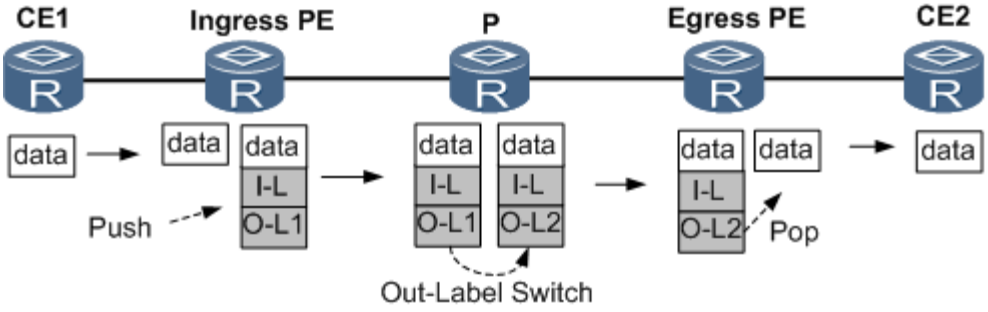
BGP/MPLS IP VPN 的基本模型由三部分组成：CE、PE 和 P：

CE（Customer Edge）：用户网络边缘设备，有接口直接与服务提供商 SP（Service Provider）网络相连。CE 可以是路由器或交换机，也可以是一台主机。通常情况下，CE“感知”不到 VPN 的存在，也不需要支持 MPLS。

PE（Provider Edge）：是服务提供商网络的边缘设备，与 CE 直接相连。在 MPLS 网络中，对 VPN 的所有处理都发生在 PE 上，对 PE 性能要求较高。

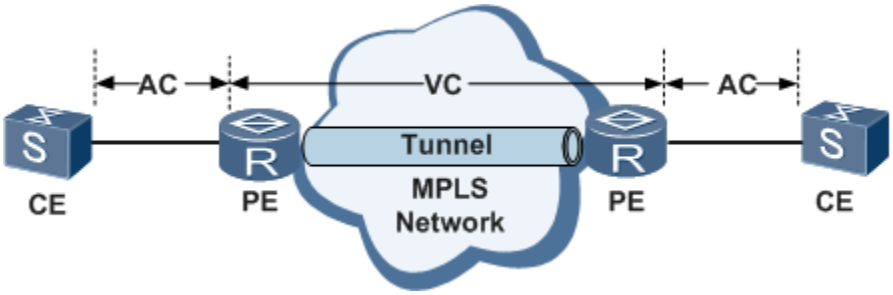
P（Provider）：服务提供商网络中的骨干设备，不与 CE 直接相连。P 设备只需要具备基本 MPLS 转发能力，不维护 VPN 信息。

在 BGP/MPLS IP VPN 骨干网中，P 设备并不知道 VPN 路由信息，VPN 报文通过隧道在 PE 之间转发。以下图为例说明 BGP/MPLS IP VPN 报文的转发过程。下图是 CE1 发送报文给 CE2 的过程。其中，I-L 表示内层标签，O-L 表示外层标签。外层标签用来指示如何到达 BGP 下一跳，内层标签表示报文的出接口或者属于哪个 VPN。



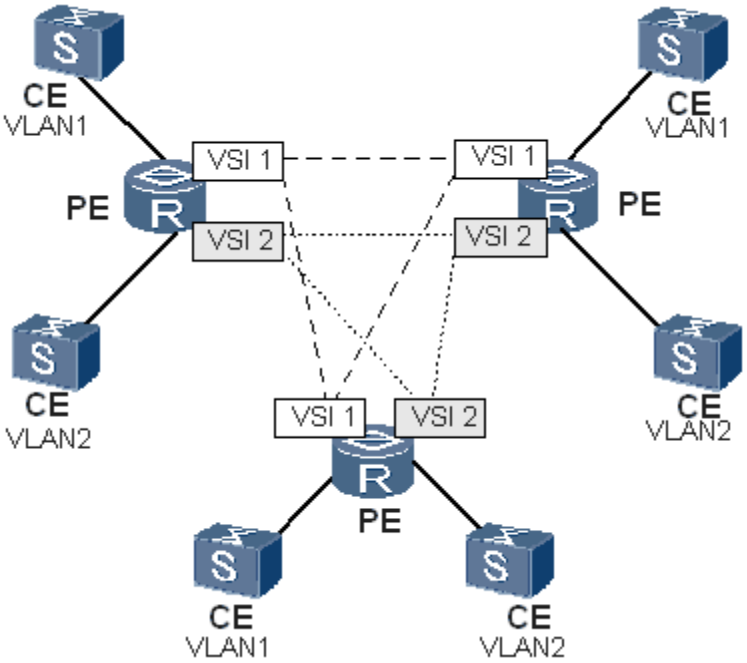
VLL

VLL 是对传统租用线业务的仿真，使用 IP 网络模拟租用线，提供非对称、低成本的 DDN（Digital Data Network）业务。从虚拟租用线两端的用户来看，该虚拟租用线近似于传统的租用线。VLL 技术是一种点到点的虚拟专线技术，能够支持几乎所有的链路层协议。



VPLS

VPLS 的主要目的就是通过分组交换网络 PSN 连接多个以太网 LAN，使它们像一个 LAN 那样工作。VPLS 可以实现多点到多点的 VPN 组网，利用 VPLS 技术，服务提供商可以通过 MPLS 骨干网向用户提供基于以太的多点业务。使用 MPLS 的虚链路作为以太网桥链路的 VPLS 解决方案，可以通过 MPLS 网络提供透明传输的 LAN 服务。



2.3.5 因特网接入

因特网接入技术丰富，分支可以根据业务需求选择不同的接入技术实现与总部的互联。

IPSEC VPN

IPSec 是 IP 层的安全技术，它在数据层面通过 AH 和 ESP 提供安全性，在控制平面使用 IKE 协议进行安全参数的协商，包括报文封装方式(AH，ESP，AH+ESP)、模式(传输模式或隧道模式)、认证算法、加密算法、密钥等。

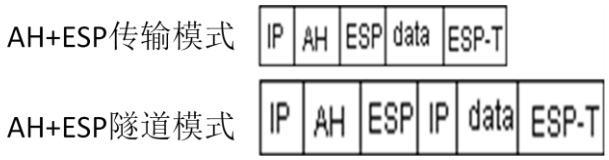
AH 即认证头，它将对原始 IP 报文采用 MD5 或者 SHA1 算法进行计算的结果作为认证数据添加到原始报文的 IP 头之后，提供对 IP 报文的无连接完整性和数据源认证，

并通过 AH 头中的序列号提供防重放攻击功能。需要注意的是，AH 不提供数据加密功能。

ESP 称为封装安全载荷，它将用户数据加密后放到 IP 报文中，为 IP 报文提供完整性检查、认证和加密功能，其中认证功能是可选的。与 AH 保护整个 IP 报文，包括 IP 头不同，ESP 仅保护 IP 头的净荷部分。ESP 支持的加密算法包括 3DES、DES、RC5、AES 等，支持的认证算法包括 MD5 和 SHA。

无论是 AH 还是 ESP，都有两种模式：传输模式和隧道模式。传输模式主要用于主机之间的通信，不会添加新的 IP 头；隧道模式主要用于网络之间的通信，会在原始报文的外面添加新的 Ip 头。

ESP 的 AH 和 ESP 可以单独使用，但因为 ESP 不能提供对 IP 头的保护，AH 不支持数据加密，因此如果既保护 IP 头、又要进行数据加密，就要同时使用 AH 和 ESP，此时一般不使 ESP 的认证功能。同时使用 AH 和 ESP 时 IP 报文的格式如下图：



无论是 AH 还是 ESP，都需要用到不同的 hash 算法、加密算法和密钥等。IPSec 中的 SA 就是指安全协议类型(AH、ESP 还是 both)、算法(包括加密和认证算法)、算法使用的密钥等的组合。算法的静态配置是可行的，但是不够灵活；而密钥采用静态配置的方式显然是不够安全的。为此，需要有一种动态选择算法和密钥的机制。在 IPSec 中，这就是通过 IKE 来完成的

IPSEC VPN 部署考虑：

（1）组播

目前业界厂商的主流实现都是遵循较早期的 IPSec 标准，因此单纯采用 IPSec 封装的报文，无法支持组播报文的转发，也就意味着无法支持组播业务和路由协议(因为路由协议报文大都是组播报文)。为此，对于需要支持组播业务和动态路由协议的分支，不能采用纯粹的 IPSec 封装，需要采用 GRE over IPSec 的方式。

（2）NAT 穿越

分支采用 Internet 作为 WAN 连接时，一般要部署 NAT。此时如果在分支网络部署 IPSec，需要考虑 IPSec 的 NAT 穿越问题，重点注意以下几个方面：

a、AH 验证范围涵盖了整个 IP 报文，对于 IP 报文头中任何字段的修改都将导致 AH 检查失败，因为 NAT 要对 IP 头进行修改，因此使用 AH 保护的 IPSec 隧道不能穿越 NAT 网关。

b、UDP/TCP 校验和需要计算 IP 头，如果采用 ESP 加密，则 NAT 无法修改校验和，导致报文非法。在 IPV4 中，TCP 的校验和是必须的，而 UDP 的校验和是可选的，在 IPV6 中 TCP/UDP 的校验和都是必选的。为此，如果用 ESP，最好采用隧道模式，对于 IPV4，如果用传输模式，则要采用 UDP 封装。

c、主模式时如果采用预共享密钥认证，则 IKE 消息中的发起者标识采用 IP 地址，用 NAT 转换后会导致载荷中包含的地址和 IP 报文头不一致。为此，有做 NAT 穿越时，最好使用数字证书认证方式；如果采用预共享密钥认证方式，则不能使用主模式，只能野蛮模式，因为野蛮模式支持用主机名标识。

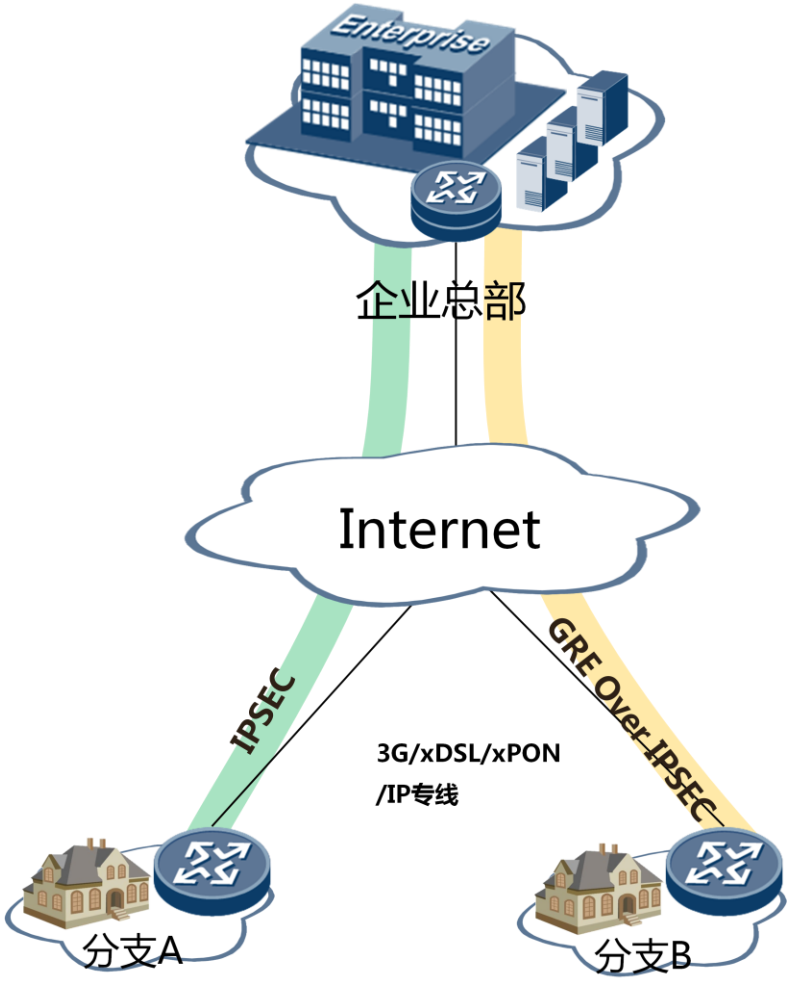
d、采用 ESP 后，原来通过检测端口号等信息实现的 ALG 功能，如 FTP 等，因为报文加密后无法再获得这些信息，将导致功能失效。

（3）对等体检测

IPSec 是对等体之间的通信，通信的建立需要 IP 可达。如果在建立会话时 IP 可达，但建立之后因为路由变化等原因不可达，IPSec 是不知道的。为此，需要有相应的检测方法。传统的检测方法是采用定期发送 Hello/ACK 报文的方式，但该方式对于需要处理大量 IPSec 会话的设备来说，CPU 负担沉重。DPD(Dead Peer Detection)检测只有在没有 IPSec 数据报文的时候才发送检测报文，极大地减少了需要 CPU 处理的协议报文数。为此，推荐采用 DPD 进行 IPSec VPN 对等体检测。

（4）报文乱序

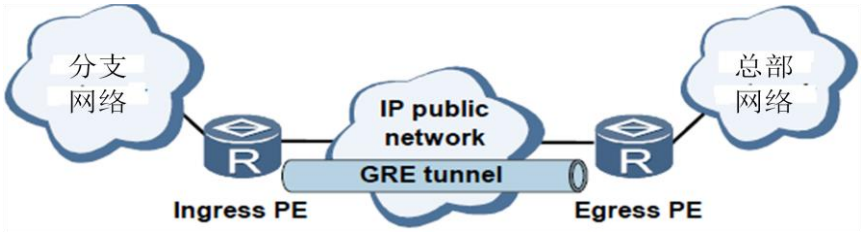
如果分支网络中同时具有多种业务，则在 WAN 口通常会采用 CBQ 等队列调度方式保证高优先级业务的优先调度。因此，如果所有报文采用一个 IPSec VPN，并不能保证所有报文在接收端是发送按序或者较小范围内的乱序到达。在这种情况下，如果使用防重放功能，很有可能导致报文在接收端被认为是具有重放攻击而被丢弃。目前我司 AR 和 S9300 上的增值业务板卡暂时不支持防重放攻击功能的关闭以及防重放窗口的调整，为此在 WAN 口流量较大，且高优先级流量比例较高的情况下，如果会出现由于队列调度导致的报文乱序在对端被认为存在防重放攻击而使报文被丢弃，就需要为不同优先级的报文分别建立 IPSec VPN。



GRE VPN

GRE 是相对较早的 VPN 方式，其基本原理就是在原有 IP 报文外面再增加一个三层报文头和一些 GRE 封装信息。

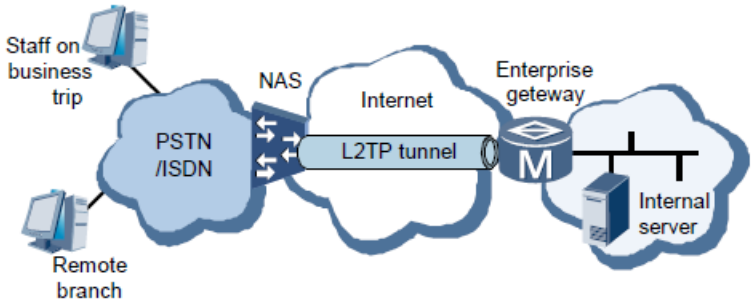
GRE 可以封装多种报文，包括 IP、MPLS 等等。对于企业网而言，如果封装 IP 报文，则外层源 IP 就是分支路由 IP，外层目的 IP 就是远端边界路由器的 IP 地址。采用 GRE 封装 IP 报文，可以在企业网内部部署 MPLS VPN，然后通过运营商的 IP 网络传输。



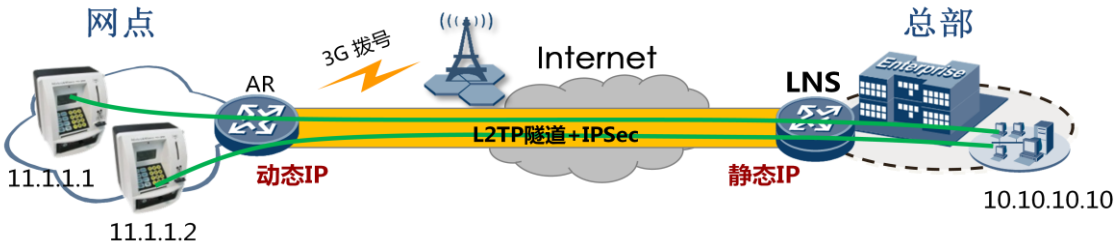
GRE 本身不提供加密和认证等安全功能，因此只适合于对数据安全没有要求的分支。如果要求保证分支数据的安全，则可以和 IPSec 结合使用，即 GRE over IPSec，通过 IPSec 对 GRE 封装报文进行加密，既提供了安全性，又解决了传统 IPSec 本身无法支撑组播业务和路由协议的问题。

L2TP VPN

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很多情况下是不现实的。L2TP 通过引入 LAC 和 LNS 解决了这一问题。



传统的 L2TP VPN，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。为了解决这种问题，另一种方式是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 PPP 的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，而且要保证分支网络的数据安全，则要和 IPSec 结合使用，即 L2TP over IPSec。



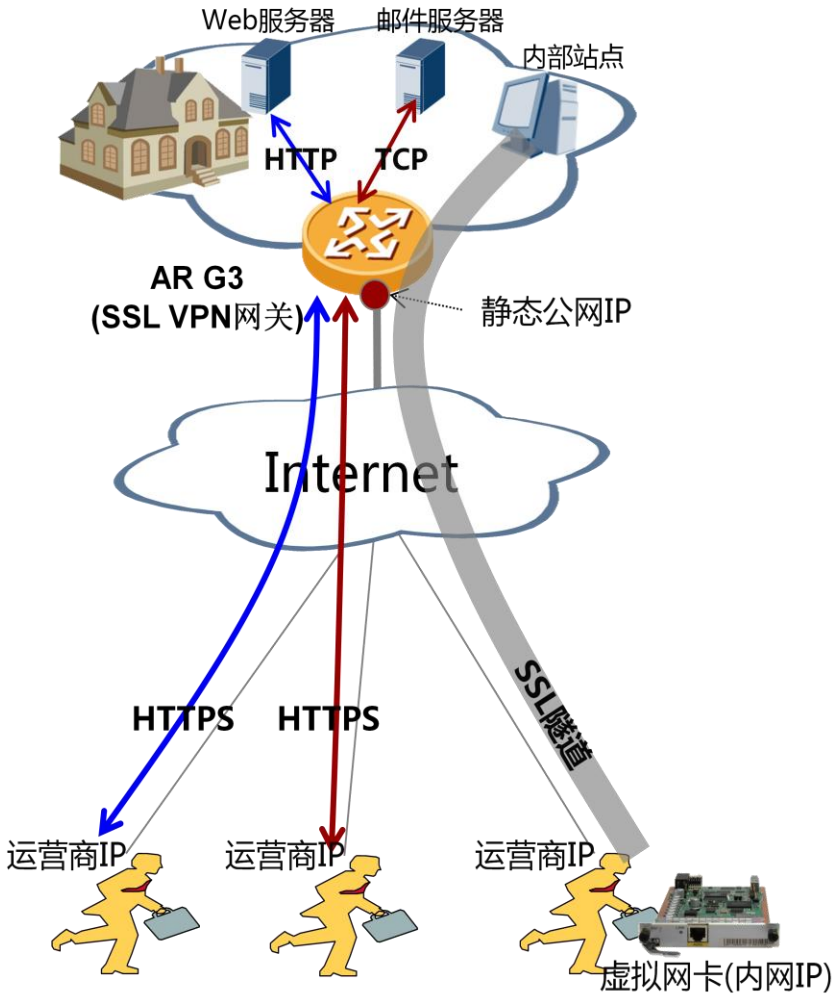
SSL VPN

SSL VPN 指的是以 HTTPS 为基础的 VPN，但也包括可支持 SSL 的应用程序，例如，电子邮件客户端程序，如 Microsoft Outlook 或 Eudora。SSL VPN 经常被称之“无客户端”，因为目前大多数计算机在出货时，都已经安装了支持 HTTP 和 HTTPS（以 SSL 为基础的 HTTP）的 Web 浏览器，所以 SSL VPN 可以通过 Web 浏览器实现无客户端的远程访问。目前，SSL 已由 TLS 传输层安全协议（RFC 2246）整合取代，它工作在 TCP 之上。如同 IPSec/IKE 一样，它必须首先进行配置，包括使用公钥与对称密钥加密以交换信息。此种交换通过数字签名让客户端使用已验证的服务器，还可选择性地通过签名或其他方法让服务器验证客户端的合法性，接着可安全地产生会话密钥进行信息 VPN 建在互联网的公共网络架构上，通过“隧道”协议，在发端加密数据、在收端解密数据，以保证数据的私密性。加密并提供完整性检查。SSL 可利用各种公钥（RSA、DSA）算法、对称密钥算法（DES、3DES、RC4）和完整性（MD5、SHA-1）算法。SSL VPN 具有如下优点：

- SSL VPN 的客户端程序，如 Microsoft Internet Explorer、Netscape Communicator、Mozilla 等已经预装在了终端设备中，因此不需要再次安装；
- SSL VPN 可在 NAT 代理装置上以透明模式工作；
- SSL VPN 不会受到安装在客户端与服务器之间的防火墙的影响。
- SSL VPN 将远程安全接入延伸到 IPSec VPN 扩展不到的地方，使更多的员工，在更多的地方，使用更多的设备，安全访问企业网络资源，同时降低了部署和支持费用。SSL VPN 正在成为远程接入的事实标准，下面列举了其中的一些理由。

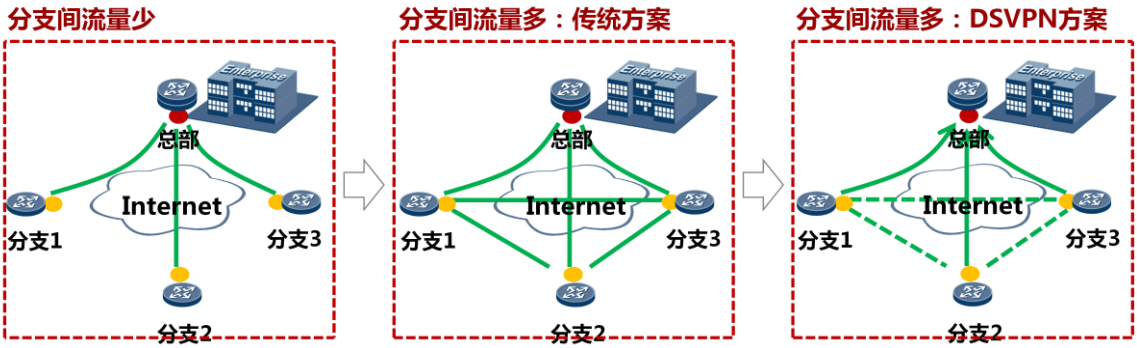
- SSL VPN 可以在任何地点，利用任何设备，连接到相应的网络资源上。SSL VPN 通信运行在 TCP/ UDP 协议上，具有穿越防火墙的能力。这种能力使 SSL VPN 能够从一家用户网络的代理防火墙背后安全访问另一家用户网络中的资源。相比 IPSec VPN 通常不能支持复杂的网络，这是因为它们需要克服穿越防火墙、IP 地址冲突等困难。鉴于 IPSec 客户机存在的问题，IPSec VPN 实际上只适用于易于管理的或者位置固定的设备。

- SSL VPN 是基于应用的 VPN，基于应用层上的连接意味着（和 IPSec VPN 比较）SSL VPN 更容易提供细粒度远程访问（即可以对用户的权限和可以访问的资源、服务、文件进行更加细致的控制，这是 IPSec VPN 难以做到的）。



DSVPN

传统的 Hub-Spoke 网络模型中，数据流量主要集中于分支与中心之间。如果分支之间有流量转发时，并应用了 IPSec 技术，中心需要在接受数据的分支隧道上解密，在发送数据的分支隧道上重新加密。分支到分支的流量跨越中心，中心 Hub 接收分支 SpokeA 的流量解密后再加密发送给分支 SpokeB，耗费了中心的资源并引入延时。通过 DSVPN 技术，分支间可动态建立数据转发通道，使分支间业务数据可以直接转发，减少了数据转发的延迟，提升了转发性能和效率。



分支间流量少：采用 Hub-Spoke 方式，分支间流量通过总部转发。基于安全考虑，总部路由器需要经过两次 IPSEC 加解密，对总部路由器压力大，且通信延时。适合分支间无流量或者流量很少的场景

分支间流量多，传统方案：分支间、分支与总部建立 IPSEC 隧道，存在 N 平方问题，组网和维护成本高。若路由器不支持 DSVPN，而且分支间流量比较多，采用此种方式。

分支间流量多，DSVPN 方案：分支与总部建立 IPSEC 隧道。分支间的 IPSEC 隧道基于流量触发，没有访问流量时不会自动建立 IPSEC 隧道，解决了 N 平方问题。DSVPN 支持 IP 组播、动态路由和 NAT 穿越。适合分支间流量比较均衡的场景。

2.3.6 分支与总部互联技术比较

互联技术	优点	缺点	适用场景
专线互联	专线专用、带宽独享。可充分保障数据传输的安全性、及时性	总体成本高、网络建设时间长，后期网络扩容、改造困难；无法满足移动办公需要	大集团、大型企业分支与总部互联，要求链路专用，对质量和安全有特别高的要求。
MPLS BGP VPN/VPLS /VLL	运营商代维管理，业务开通时间短，SLA 有保障	对于企业出口路由器规格和性能要求高，专业技术要求高	没有广域专网、对网络质量有要求的大中型分支机构与总部互联。VLL 场景适合单分支和总部互联。VPLS 场景适合多分支不仅需要访问总部，分支之间还需要互访场景。VLL 和 VPLS 基于二层转发，PE 设备不需要学习路由信息。MPLS VPN 场景与 VPLS 场景需求相同，MPLS VPN 场景基于三层路由，可以通过 RT 实现分支访问控制。
L2TP VPN	作为 PPTP 和 L2F 的替代性技术，实现简单，通用性好	缺乏数据加密机制，不适合站点间互联	适合出差员工需要到总部进行 PPP 身份认证场景，认证通过后给出差员工分配内网地址，实现与总部的互联。
GRE VPN	可以承载多种非 IP 协议	缺乏数据加密机制	总部与分支站点互联技术，但是 GRE 不能实现数据加密功能，网络传输存在安全隐患。
IPSec VPN	对于安全要求很高的用户，可提供数据认证和加密措施	不能承载路由协议，可扩展性差	分支与总部通过 Internet 实现互联的主要技术，技术成熟，应用广泛，可根据业务需求选择是否加密，但是该技术只能承载 IP 报文。
SSL VPN	端到端数据安全保障，无需 VPN 客户端	仅支持基于 WEB 的应用，文件共享及 Email。高 CPU 占用	适合客户、合作伙伴、供应商等随时随地通过 WEB 方式访问总部，不需要安装客户端。
GRE Over IPSec VPN	可承载多种非 IP 协议，支持路由协议，具备数据认证和加密措施，安全性高	报文解封装效率低	总部与分支站点互联技术，由于 IPSEC 不能承载非 IP 报文，可以通过 GRE OVER IPSEC VPN 实现非 IP 报文的承载，作为 IPSEC VPN 的有效补充技术。

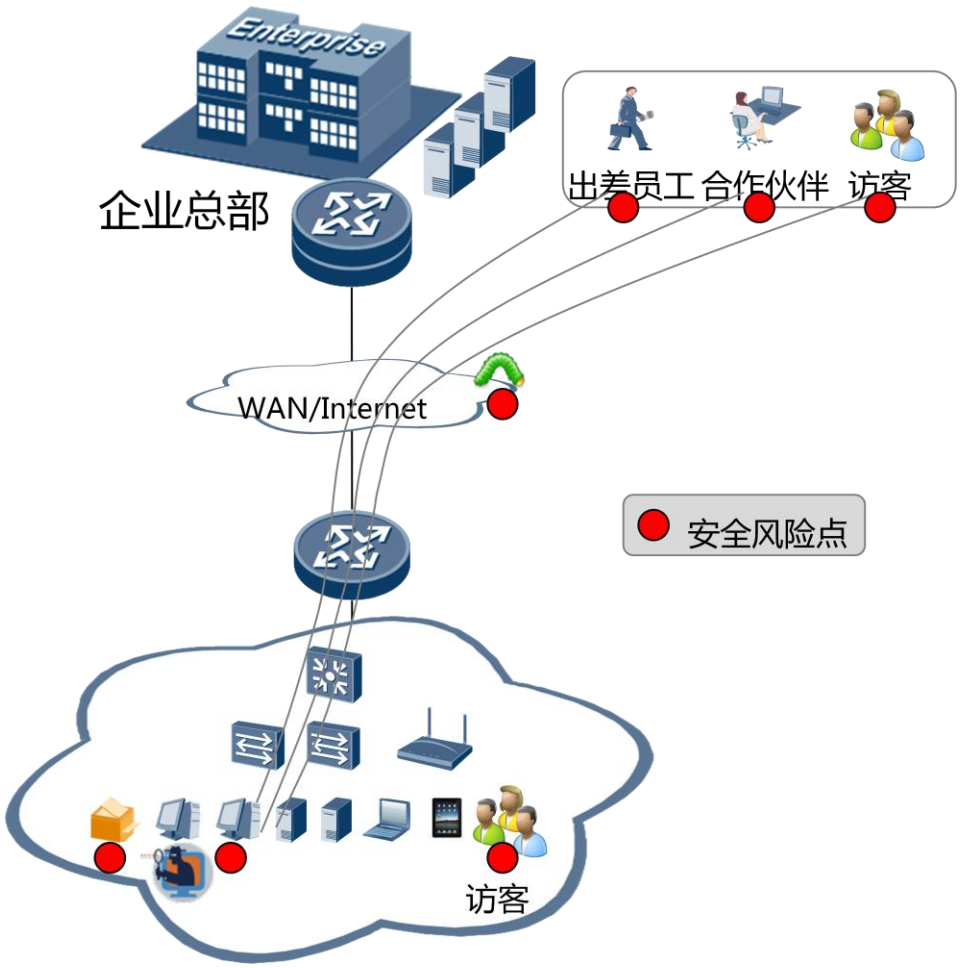
2.4 分支安全

2.4.1 分支安全挑战

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。

在分支网络，一般使用防火墙作为安全设备。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

分支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，接入安全主要指导分支内的安全接入，包括终端安全接入控制；远程接入涉及合作伙伴、出差人员对分支内部的安全访问；边界防御通过防火墙对分支出口和分支内的各个组织单元之间进行有效防护和隔离。



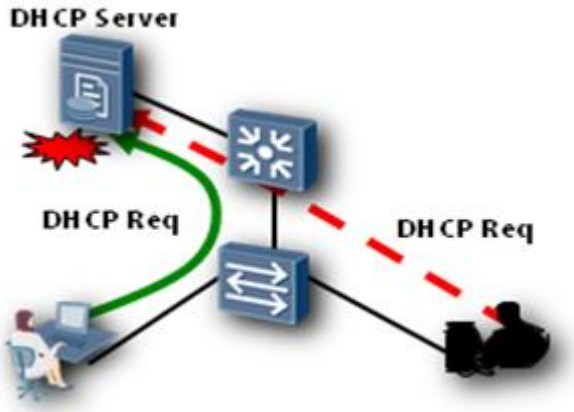
2.4.2 内网安全规划

网络的安全是分支网络安全的最基本保证。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**错误！未找到引用源。**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。



DAI-ARP 欺骗

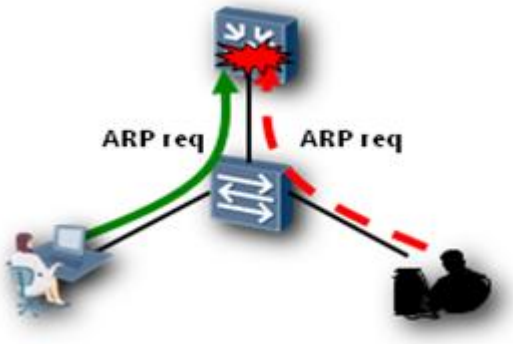
动态 ARP 检测（Dynamic ARP Inspection）应用在设备的二层接口上，利用 DHCP Snooping 绑定表来防御 ARP 攻击。当设备收到 ARP 报文时，将此 ARP 报文中的源 IP、源 MAC、端口、VLAN 信息和 DHCP Snooping 绑定表的信息进行比较。如果信息匹配，说明是合法用户，则允许此用户的 ARP 报文通过；否则，认为是攻击，丢弃该 ARP 报文。

如**错误！未找到引用源。**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。

下图给出了 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。



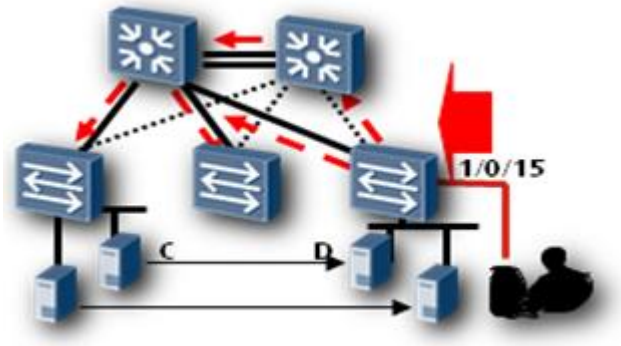
MAC 泛洪

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。下图给出了 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。



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。

如**错误！未找到引用源。**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

分支网络中，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。

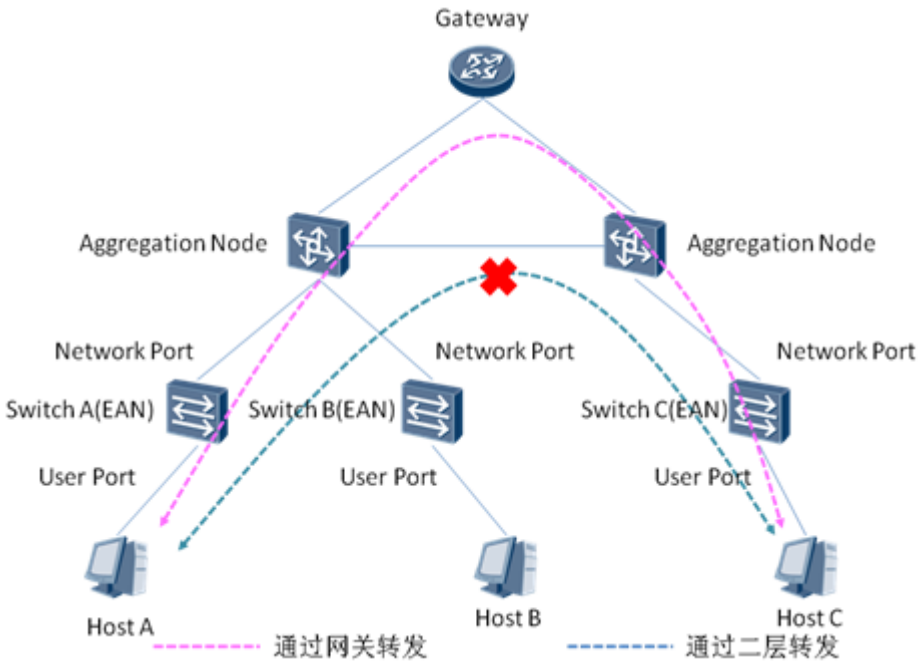
- 网络接口

  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：

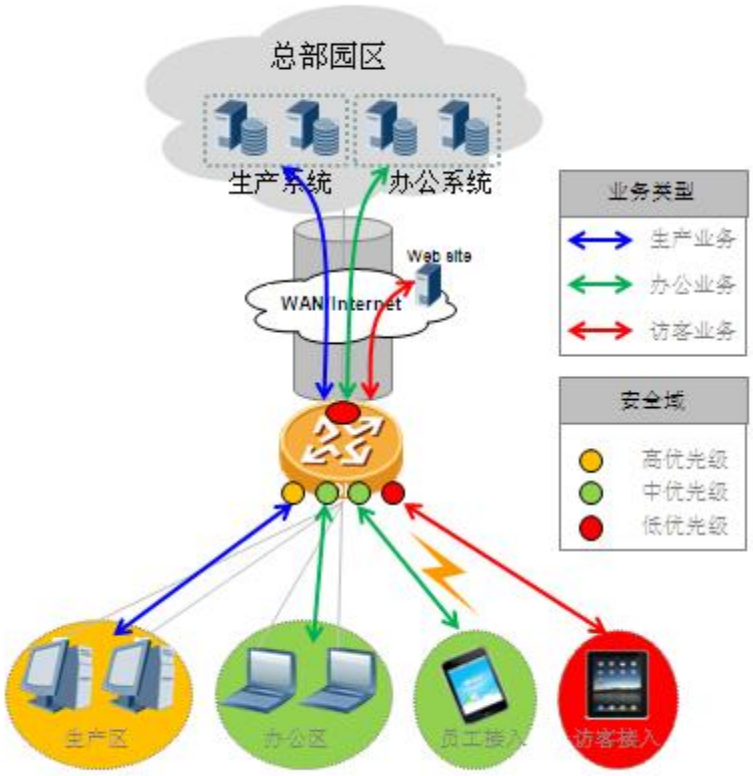
  - 允许组播报文和 DHCP 报文通过。
  - 对于 ARP 报文则上送 CPU 进行处理。
  - 其他广播报文都不允许通过。

下图给出了 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。



生产/办公网隔离

在分支进行安全域的划分，分支生产/办公网划归不同 VLAN，并且加入高/中优先级安全域，员工无线接入/访客无线接入使用不同 SSID，分别加入中/低优先级安全域，将设备出口链路加入低优先级安全域。安全域默认规则为高优先级区域可以访问低优先级区域，低优先级区域访问高优先级区域通过配置控制。在分支进行 ACL 的访问控制，控制开放生产区和生产系统服务器、开放办公区和办公系统服务器、无线员工接入和办公系统服务器、无线访客接入和 Internet 之间的访问控制，提升分支内的业务安全性。

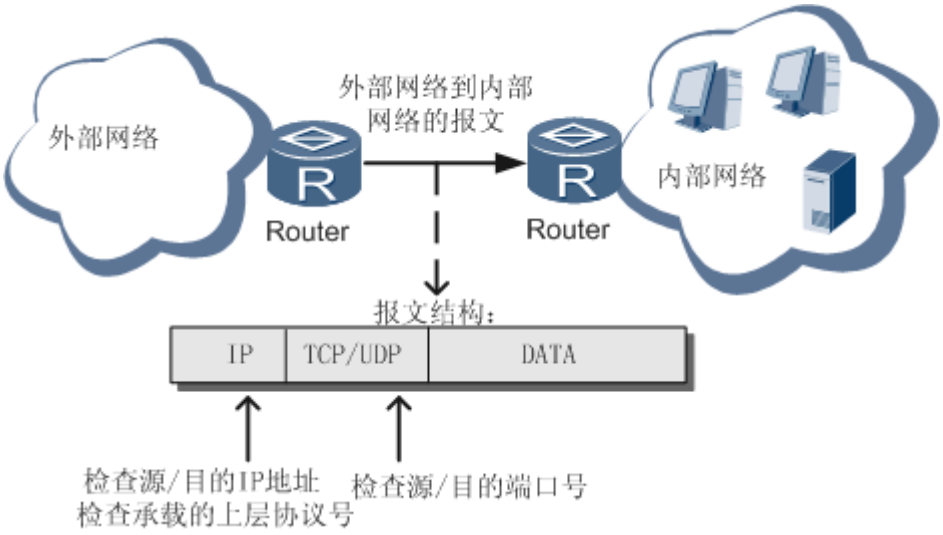


2.4.3 集成防火墙外网安全规划

在中小型企业分支，我们推荐采用 AR G3 集成防火墙功能来进行外网安全规划，通过包过滤防火墙、ASPF、攻击防范等技术实现分支的安全。

包过滤防火墙

包过滤防火墙的基本原理是：通过配置 ACL 实施数据包的过滤。实施过滤主要是基于数据包中的 IP 层所承载的上层协议的协议号、源/目的 IP 地址、源/目的端口号和报文传递的方向等信息。包过滤应用在路由器中，对路由器需要转发的 IP 数据包，先获取数据包的包头信息，然后和设定的 ACL 规则进行比较，根据比较的结果决定对数据包进行转发或者丢弃。



ASPF

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。Eudemon 系列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 命令字、SMTP 命令的检测、HTTP 的 Java、ActiveX 控件等的检测。

ASPF 技术是在基于会话管理的技术基础上提供深层检测技术的，ASPF 技术利用会话管理维护的信息来维护会话的访问规则，通过 ASPF 技术在会话管理中保存着不能由静态访问列表规则保存的会话状态信息。会话状态信息可以用于智能的允许/禁止报文。当一个会话终止时，会话管理会将该会话的相关信息删除，防火墙中的会话也将被关闭。

针对 TCP 连接，ASPF 可以智能的检测“TCP 的三次握手的信息”和“拆除连接的握手信息”，通过检测握手、拆连接的状态检测，保证一个正常的 TCP 访问可以正常进行，而对于非完整的 TCP 握手连接的报文会直接拒绝。

攻击防范

网络攻击一般分为拒绝服务型攻击、扫描窥探攻击和畸形报文攻击三大类：

1、拒绝服务型 DoS（Denial of Service）攻击是使用大量的数据包攻击系统，使系统无法接受正常用户的请求，或者挂起不能正常的工作。主要 DoS 攻击有 SYN Flood、Fraggle 等。拒绝服务攻击和其他类型的攻击不同之处在于：攻击者并不是去寻找进入内部网络的入口，而是阻止合法用户访问资源或路由器。

2、扫描窥探攻击是利用 ping 扫描（包括 ICMP 和 TCP）来标识网络上存活着的系统，从而准确地指出潜在的目标。利用 TCP 和 UDP 等进行端口扫描，就能检测出操作系统的种类和潜在的服务种类。攻击者通过扫描窥探就能大致了解目标系统提供的服务种类和潜在的安全漏洞，为进一步侵入系统做好准备。

3、畸形报文攻击是通过向目标系统发送有缺陷的 IP 报文，使得目标系统在处理这样的 IP 包时会出现崩溃，给目标系统带来损失。主要的畸形报文攻击有 Ping of Death、Teardrop 等。

2.4.4 专业防火墙外网安全规划

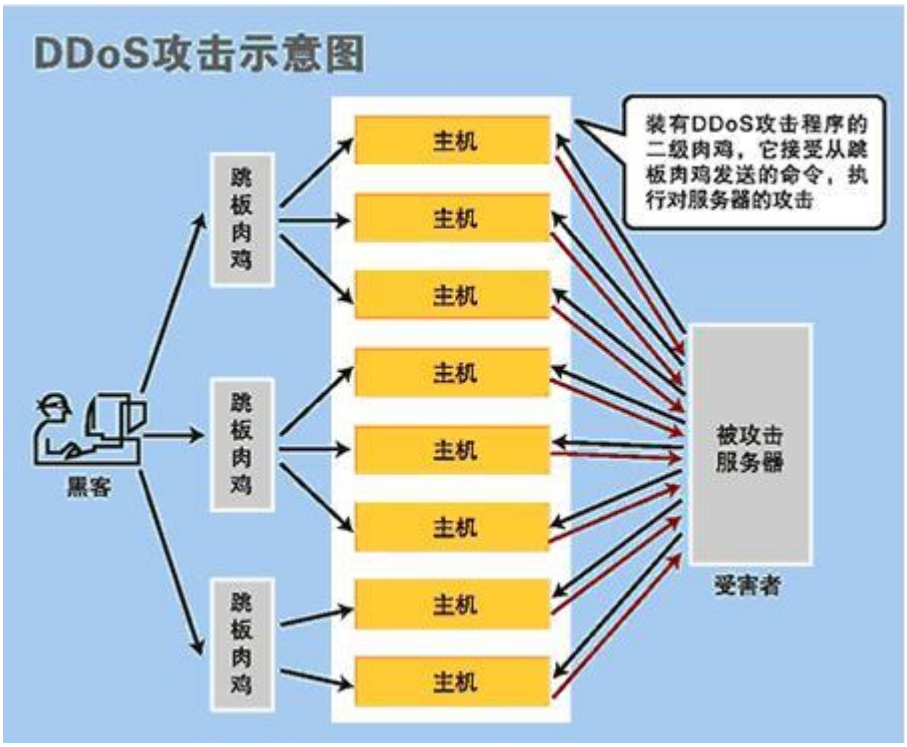
在对安全等级要求高的大中型企业分支，我们推荐采用 Eudemon 专业防火墙功能来进行外网安全规划。Eudemon 防火墙除了支持基本防火墙功能外，还可以通过如下功能实现更高安全等级的安全防护。

DDoS 防御

DDoS（Distributed Denial Of Service）把 DoS 又向前发展了一大步，这种分布式拒绝服务攻击是黑客利用在已经侵入并已控制的不同的高带宽主机（可能是数百，甚至成千上万台）上安装大量的 DoS 服务程序，它们等待来自中央攻击控制中心的命令，中央攻击控制中心在适时启动全体受控主机的 DoS 服务进程，让它们对一个特定目标发送尽可能多的网络访问请求，形成一股 DoS 洪流冲击目标系统，猛烈的 DoS 攻击同一个网站。在寡不敌众的力量抗衡下，被攻击的目标网站会很快失去反应而不能及时处理正常的访问甚至系统瘫痪崩溃。可见 DDoS 与 DoS 的最大区别是人多力量大。DoS 是一台机器攻击目标，DDoS 是被中央攻击中心控制的很多台机器利用他们的高带宽攻击目标，可更容易地将目标网站攻下。另外，DDoS 攻击方式较为自动化，攻击者可以把他的程序安装到网络中的多台机器上，所采用的这种攻击方式很难被攻击对象察觉，直到攻击者发下统一的攻击命令，这些机器才同时发起进攻。可以说 DDoS 攻击是由黑客集中控制发动的一组 DoS 攻击的集合，现在这种方式被认为是最有效的攻击形式，并且非常难以抵挡。

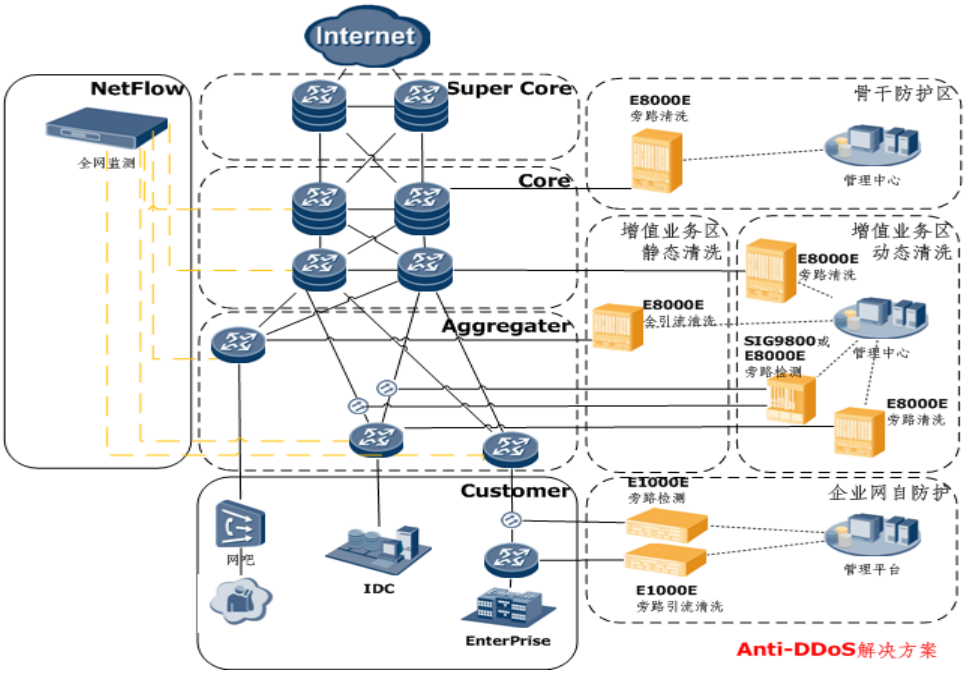
被攻击主机上有大量等待的 TCP 连接，导致网络中充斥着大量的无用的数据包，源地址是假的。攻击者制造高流量无用数据，造成网络拥塞，使受害主机无法正常和外界通讯。利用受害主机提供的服务或传输协议上的缺陷，反复高速的发出特定的服务请求，使受害主机无法及时处理所有正常请求。严重时会造成系统死机。

Botnet僵尸网络是攻击者利用互联网秘密建立的、可以集中进行控制的计算机集群，通常包括被植入“僵尸”程序 Bot 的计算机集群（Zombie）、一个或者多个控制器（通常利用互联网中的公共服务器）、控制者终端（攻击者发出控制指令的地方）。Botnet 由于隐蔽性强、危害巨大、难以追查和清除，正在逐渐成为一个平台，当前危害最大的 DDoS 攻击、垃圾邮件等多是利用 Botnet 发起的。



DDoS攻击模型

DDoS 解决方案如下：



1．攻击检测：城域网内部采集 Netflow 信息或者采用 SIG9280E，通过流量建模，有效识别各种异常流量，判断出 DDoS 攻击发生情况。
2．攻击告警：确定有异常流量攻击后，向清洗中心设备发出攻击告警；
3．路由器协调：清洗中心设备根据流量检测结果，向上联设备发送关于被攻击网段或者主机的路由通告，指出到达被攻击网段的下一跳地址是清洗设备的地址；
4．流量牵引：将原来去往被攻击目标 IP 的流量牵引至旁路抗清洗设备。被牵引的流量为攻击流量与正常流量的混合；
5．攻击防护及流量清洗：混合流量到达清洗设备后，通过多层的攻击流量识别与净化功能，将 DDoS 攻击流量从混合流量中分离、过滤，而使正常流量顺利通过；
6．流量注入：经过清洗设备净化之后的合法流量被重新注入回网络，到达目的 IP。此时从服务器看，DDoS 攻击已经被抑止，服务恢复正常；
7．正常流量未受干扰：从整个自动防护的过程来看，其他去往未受攻击服务器的合法流量，依然按原路由到达目的地，正常业务未受任何干扰。
在流量清洗中心的部署完成与初始的配置之后，异常流量清洗系统整个工作过程都可以自动完成，无须人为干预。从攻击检测到流量牵引、清洗防护的过程反应迅速，而对管理员来说管理简单便捷，只需要进行过程监控工作，大大提高集中接口的稳定性和可用性

蠕虫病毒防范

蠕虫病毒主要由三部分构成：
1、病毒传播。蠕虫病毒具有自动利用网络传播的特点，正是由于这个特点导致蠕虫病毒成为了现在网络中面临的一个巨大的问题。在病毒的传播的同时，也造成了带宽的极大浪费，严重的情况可能会造成网络的瘫痪。
2、病毒隐藏。病毒隐藏是所有病毒的基本特征，通过在主机上隐藏，使得用户不容易发现病毒的存在。
3、控制模块，该模块通过后台运行，进一步感染其他主机或者打开系统的某些后面，以达到控制主机的功能。
按照蠕虫病毒的构成特点，在网络中应该重点关注病毒传播部分，因为只要在网络中隔断了病毒的传播，就可以很大程度上抑制了病毒的泛滥，有效的保证了网络的安全运行。而根据病毒的隐藏合控制特征，可以更新主机病毒杀毒软件，通过病毒的特征码发现在主机上面的问题。

传统的蠕虫病毒可以依靠如下两种方式防范：
1、 使用主机安装的杀毒软件，针对病毒本身的特征码识别病毒，查杀病毒。这种方式有一个很大的问题是，由于是被动的防御式清除病毒，因此当刚刚查杀病毒之后，如果连接到网络上之后，立刻可能又被感染病毒。造成杀毒、染毒周而复始不能彻底的解决问题。
2、 针对蠕虫病毒的攻击漏洞，我们及早发现，及时的打上安全补丁，这样可以防止蠕虫病毒的入侵。

上述方法的一个不完善的地方是，虽然保护了主机自身的安全，但是网络已经被破坏了。因此我们需要从网络整体来考虑如何防范蠕虫病毒的传播，隔断了传染源，不但可以保护其他主机免受侵害，同时还可以保证整个网络的正常运行。

因为蠕虫病毒传播的一个重要特征就是通过扫描方式发现具有漏洞的主机，从而进一步感染主机。因此防火墙要发现蠕虫病毒传播的行为，首先要具有发现扫描行为的能力。因此，需要具有识别正常报文和扫描报文的能力。
当发现了一个主机进行扫描的时候，必须具有一定针对性的策略以防止扫描报文对防火墙系统造成的系统消耗。因为在发现扫描攻击的过程中，必定会漏掉部分的报文，因此如果没有后续的防范策略，依然无法正常的防范蠕虫病毒的传播。

Eudemon 系列防火墙具有先进的扫描防御能力，可以有效的发现 IP 扫描、TCP/UDP 端口扫描等各种扫描行为。

扫描类一般分为端口扫描和地址扫描：
地址扫描类攻击一般采用如下的方式进行：运用 ping 这样的程序探测目标地址，对此作出响应的表示其存在，用来确定哪些目标系统确实存活着并且连接在目标网络上。也有可能使用 TCP/UDP 报文对一定地址发起连接（如 TCP ping），判断是否有应答报文。
端口扫描类攻击一般采用如下的方式进行：向大范围的主机的一系列 TCP/UDP 端口发起连接，根据应答报文判断主机是否使用这些端口提供服务。
Eudemon 系列防火墙通过特点的算法，可以有效的检查出扫描行为的发生，对于发现以后的扫描报文进行丢弃，并进行日志记录。

当发现了一个主机进行了扫描攻击行为之后，如果不采取进一步的智能防范措施，依然无法防止蠕虫病毒的传播。扫描过程是持续不断的，在扫描监控的过程中会有部分的报文通过防火墙的，因为扫描必须达到一定的累计量才能确认是扫描行为，如果仅仅发现扫描攻击是不够的。
Eudemon 系列防火墙在发现扫描攻击以后会采用如下一些策略防止蠕虫病毒的扩散：
1、当发现扫描攻击之后，首先丢弃扫描攻击发现以后的报文，同时把产生扫描行为的主机加入到黑名单，加入黑名单的具体时间是可以调整的。
2、当主机加入到黑名单之后，该主机的访问就会自动的受到黑名单的控制，这样即使是新开始的扫描行为依然逃脱不了防火墙的监控。
3、某些主机加入到黑名单以后，也不能完全阻挡这个主机发出的所有报文，因为如果阻挡所有的报文，会造成用户的上网等受到影响，因此还不能完全阻挡这个主机的所有报文。Eudemon 系列防火墙还提供了“白名单”的技术，通过预先设定的策略可以智能的判断应该丢弃哪些报文、允许哪些报文。
4、Eudemon 防火墙内置了病毒策略引擎，可以动态的发现已知蠕虫病毒。同时 Eudemon 防火墙可以提供 WEB 重定向的功能，可以引导染毒用户到对应的补丁站点或者是杀毒站点，针对病毒源头进行处理

攻击防范

丰富的 DoS 防御：
Eudemon 防火墙产品根据数据报文的特征，以及 Dos 攻击的不同手段，可以针对 ICMP Flood、SYN Flood、UDP Flood 等各种 Dos 攻击手段进行 Dos 攻击的防御。
同时，Eudemon 防火墙可以主动识别出数十种常见的攻击种类，很多种攻击种类造成的后果就是 Dos 形式的攻击，Eudemon 防火墙可以主动发现并隔断这些非法攻击，消除了内部网络遭受攻击的可能。通过对各种攻击的防御手段，利用 Eudemon 防火墙可以组建一个安全的防御体系，保证网络不遭受 Dos 攻击的侵害。
针对不同的攻击特点，Eudemon 防火墙采用了一些不同的防御技术，这样保证 Eudemon 防火墙在抵御 Dos 攻击的时候更有针对性，使得整个 eudemon 防火墙的抵御特性更加完整。
Eudemon 防火墙不但在攻击手段上面进行了详细考虑，同时也在使用方式和网络适应性方面做了周全的考虑，攻击防范既可以针对一台特定的主机也可以针对一个安全区域的所有主机进行保护。

高级的 TCP 代理防御体系：Eudemon 系列防火墙支持使用 TCP 代理方式来防止 SYN Flood 类的 Dos 攻击，这种攻击可以很快的消耗服务器资源，导致服务器崩溃。在一般的 Dos 防范技术中，在攻击发生的时候不能准确的识别哪些是合法用户，哪些是攻击报文。Eudemon 防火墙采用了 TCP 透明代理的方式实现了对这种攻击的防范，Eudemon

防火墙通过精确的验证可以准确的发现攻击报文，对正常报文依然可以通过允许这些报文访问防火墙资源，而攻击报文则被 Eudemon 防火墙丢弃。
有些攻击是建立一个完整的 TCP 连接用来消耗服务器的资源。Eudemon 系列防火墙可以实现增强代理的功能，在客户端与防火墙建立连接以后察看客户是否有数据报文发送，如果有数据报文发送防火墙再与服务器端建立连接否则丢弃客户端的报文。这样可以保证即使采用完成 TCP 三次握手的方式消耗服务器资源，也可以被 Eudemon 防火墙发现

ARP 攻击防御：在设备的接口下，挂着一些计算机，有些用户，会恶意的伪造其它设备的 IP 地址，发 ARP 报文，网关设备因为无法识别这些 ARP 报文的真伪，可能会根据这些报文更新 ARP 表，导致接口上的 ARP 表里，IP 和 MAC 地址正确的对应关系被修改，这会导致部分计算机不能上网，只有当 ARP 表项被老化或者这些计算机重新启动后（启动后会发免费 ARP 报文，导致网关设备会重新更新成正确的 IP 和 MAC 对应关系表），才能恢复上网。只要 ARP FLOOD 攻击在不断进行，就会有大量用户被攻击下线，这也是比较常见的 DoS 攻击方式。
Eudemon 防火墙针 IP 和 MAC 地址解析映射关系，通过对地址解析请求报文进行确认，以保证 IP 和 MAC 地址映射关系正确性。在运行地址解析协议的设备接收到地址解析协议请求报文之后，根据该请求报文中所携带的请求者的 IP 地址再次构造地址解析协议请求报文，向广播网络内发送，请求原有请求报文中请求者的硬件地址。如果收到了对这个请求的地址解析协议应答报文，则可以确认这个地址映射关系的真实性；如果在一定时间之内没有收到对这个请求的地址解析协议应答报文，则认为原来收到的地址解析协议请求报文为错误的或伪冒的报文，根据这个报文产生的地址映射关系是错误的，不能作为数据报文在物理网络上转发的依据。通过对 ARP 解析的精确识别，保证了在二层网络中 ARP 表项的安全。

上网行为管理

随着信息技术和互联网的深入发展，互联网日益成为人们工作、学习和生活的一部分。在享受互联网带来的巨大便利的时候，由其带来的负面影响和安全威胁也日趋严重；复杂的互联网使用环境也带给管理者诸如组织成员工作效率降低、带宽资源滥用、信息机密外泄等问题，并因此而产生法律、安全等问题。企业分支管理者对互联网管理，上网行为规范和提高网络利用率等方面提出了迫切的需要。

1、多种接入方式：Eudemon可为用户提供多种接入方式，其中包括旁路接入，透明/路由方式的接入。
旁路接入：对现有网络应用和网络拓扑不产生任何影响，不占用网络带宽。隐藏 IP 模式，用户无法发现系统，更无法攻击系统。
透明/路由：透明模式，不改变网络拓扑结构；路由模式中还支持源及目标地址转换，最大程度满足用户接入需求。
2、基于用户的四层行为管理：为用户提供了四个层次的行为控制：第一层接入控制采用实名制及IP 管理，这种管理方式，使得用户名与IP 地址、MAC地址实现统一规划和捆绑，未通过系统认证管理的用户禁止进入网络环境，极大保护了用户网络环境的安全。第二层网络权限控制当用户通过网络接入允许的认证后，系统开始控制访问网络的协议

及相关资源，并对应用带宽进行限制，网络中所有用户必须按照该限制进行网络访问。第三层协议及应用控制当用户通过前两层控制后，此时系统对应用协议和应用软件进行控制，这些控制包括了IM 聊天、P2P 下载、收发邮件、URL 访问、网游、股票等等一系列应用。第四层应用内容控制当前用户行为都经过了前三层的应用控制后，接下来再对应用内容进行控制，其中包括了BBS 发帖的内容、博客中的内容、聊天的内容、邮件中包含的内容等等进行控制。这种多层次的行为管理控制不但为用户提供了详细的可视化审计、还为用户提供了详实的行为控制，真正实现了多层次的用户管理。

3、IP/MAC 自动探测、绑定：IP/MAC 自动探测绑定功能是网络接入及控制中非常实用的功能，这种自动探测和绑定降低了网络管理员面对大量用户数的网络环境实现绑定时的难度和工作量，真正做到了人性化的网络管理。

4、实时的活动监控：能够实时监控用户的网络活动，并能将用户的上网活动生成清晰的数据报表。例如可以实时监控活动用户的每一个会话连接，并能够准确识别出每一个会话所属应用类别；可以实时监控所有用户的网络活动，并生成数据统计报表；可以实时监控每一网络接口的流量状态，并生成动态折线图。

5、详细的带宽控制：能够针对用户/用户组、IP/IP 段、应用/应用组等对象来进行上/下行速度、连接数、连接速率以及时间等多方面的带宽控制。例如针对P2P 应用，如果要针对某一个IP 段设置策略，希望控制其在上班时间的P2P 下载，那么可以针对该IP 段设置希望控制的上/下行速率、设置策略在上班时间生效(如9:00～12:00、13:00～18:00)，另外还可以根据情况设置该IP 段中各个IP 的连接数、发起连接的速率等来进一步限制该IP 段中每一IP 的P2P 下载。并可实时查看用户带宽使用情况。

6、详细的内容审计：能够对 SMTP、POP、WebMail、BBS、MSN、飞信、Yahoo 通等等多种能够发送具体内容的应用进行内容审计。例如对BBS 发帖的监控，一旦开启了对用户BBS 发帖（网页提交）的监控，那么无论用户在论坛、新闻评论、网络社区等发布任何信息，设备都可以完整的对这些内容进行审计记录，并可针对关键字进行报警。

7、内容回放功能：能够将用户的网络行为完整的记录下来，进行事后的回放。例如对于SMTP、POP 等邮件，可以完整的记录邮件的收、发件人、发件时间、主题甚至内容和附件，管理员可以根据这些记录的内容来回放用户的这些行为。支持网页的内容回放功能。

8、丰富的应用识别分类：识别多种协议和应用，总计近 200 种。系统可以识别P2P 共计12 种，并可以智能识别其它未分类P2P；IM 识别8 种；文件传输识别9 种；流媒体2 种；E-Mail 共计6 种；webMail 共计16 种；网络游戏共计21 种；网页游戏共计17 种；炒股软件大类7 种，但如大智慧包含了国泰君安大智慧、银河证券大智慧等多个版本，统计这些分类可达26 余种；网络电视21 种；地下浏览6 种；BBS 发帖可以针对经过验证的500 多个论坛、社区、新闻网站进行监控；网络电话2 种；其它常用网络协议80余种。

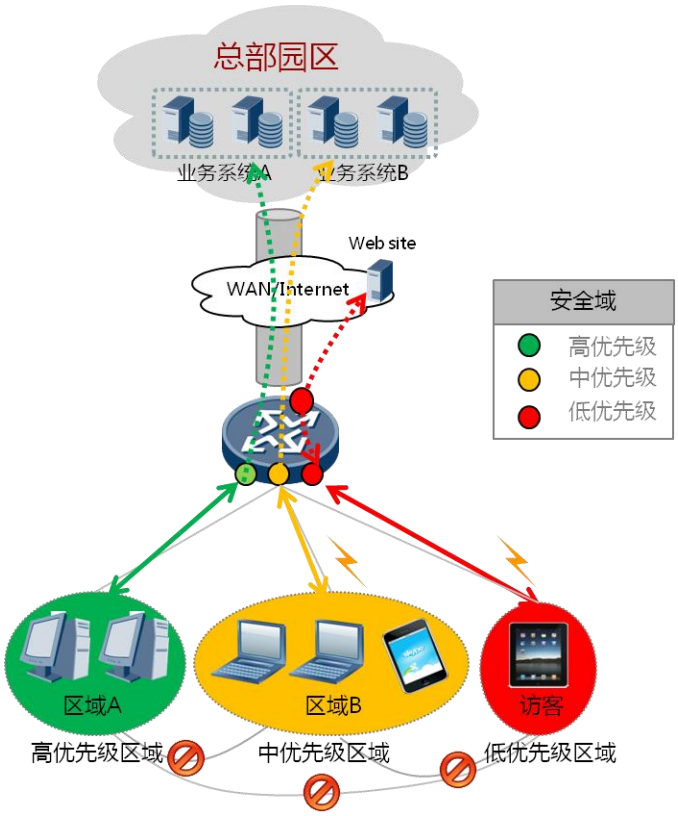
9、丰富全面的网络应用协议库：能够对标准应用协议，如：电子邮件、P2P、IM 即时通信、网络游戏、网络电视、在线炒股、流媒体、远程登录、代理软件等200 多种网络应用进行准确的识别与控制。

10、实时维护，定期更新：随着互联网的迅速普及，各种网络应用层出不穷，而且版本更新速度越来越快。天融信的专业的应用协议分析团队实时跟踪网络应用的变化情况，在第一时间内提供升级包，用户可以设置定期下载更新。

2.4.5 AR 集成防火墙部署规划

内网区域隔离

AR 自身集成防火墙功能，并且分支内部网络划分不同安全等级的区域，通过部署区域隔离功能，不同安全级别的区域互访得到控制。内网区域隔离适用于小/微型分支，尤其是对安全性要求高的金融场景。如生产/办公网/访客之间隔离。



（1）采用 AR 路由器集成的安全域特性实现 。

（2）高优先级区域可以无阻碍访问低优先级区域 。

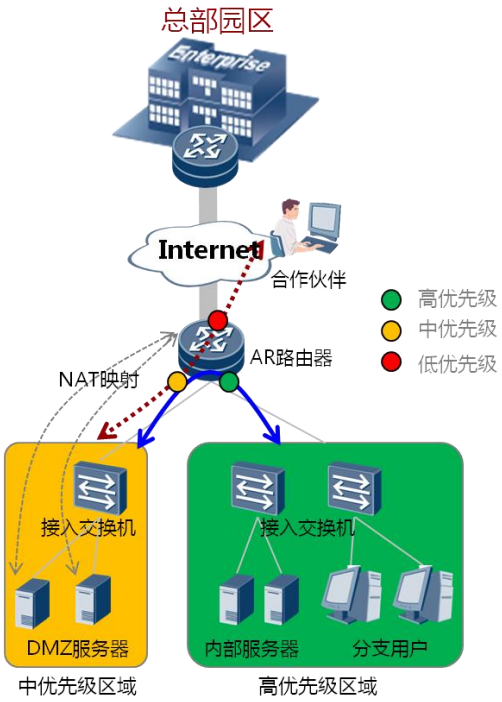
（3）低优先级区域访问高优先级区域需配置。

（4）分支内不同部门归属不同 vlan，对应 vlanif 加入不同安全域。

（5）分支因特网出口与访客加入低优先级域。

分支 DMZ 服务部署

如果分支网络跟合作伙伴之间有业务往来的需求，则建议在分支内部建议 DMZ 区域，提供合作伙伴的安全接入。内含 DMZ 服务器的中型分支，只向合作伙伴开放 DMZ 服务器，而不向公众开放的场景，适合采用 AR 集成防火墙，通过划分安全域解决。



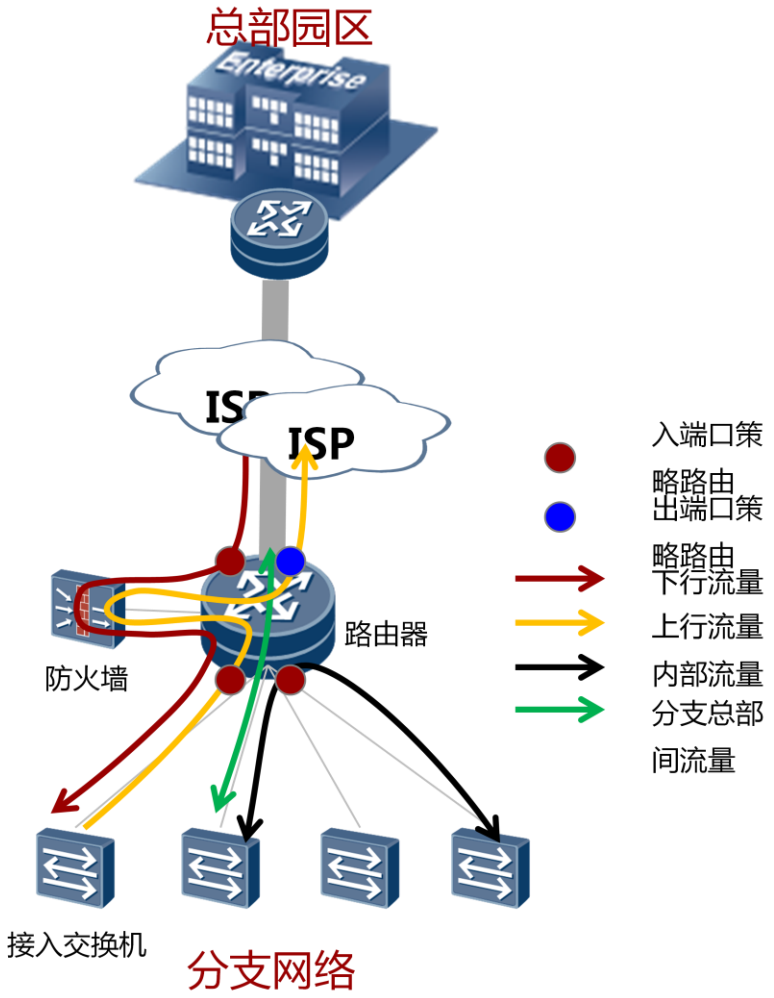
（1）DMZ 服务器连接到 AR 路由器的 DMZ 区域 。

（2）DMZ 服务器通过接入交换机或直接挂接到 AR 路由器，AR 作为其三层网关。

（3）DMZ 服务器采用私网 IP 地址，出口路由器将其固定映射到公网 IP。

2.4.6 专业防火墙部署规划

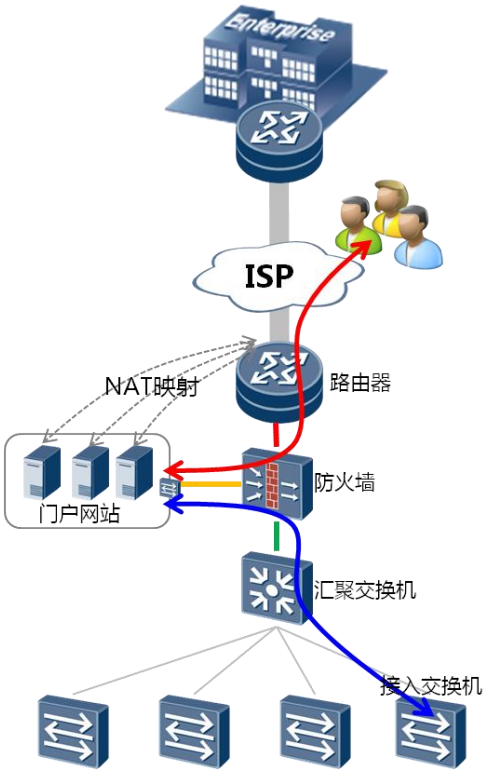
防火墙旁路部署



防火墙旁挂在出口路由器旁，防火墙工作于路由模式。路由器下联口的入方向配置策略路由，分支内部流量本地三层转发，不经过防火墙；分支与总部流量间流量封装进IPSEC隧道，不经过防火墙；分支其他流量（上网流量）重定向到防火墙。路由器上联口的入方向配置所有流量重定向到防火墙。本方案通过防火墙旁挂，出口路由器直连接入交换机，可以省略汇聚交换机，简化网络架构。

采用防火墙旁路部署，适用于对于内部有门户网站的大/中型分支，对安全要求比较高，单纯采用AR集成防火墙无法阻止来自因特网的攻击，须采用专业防火墙做安全隔离。

防火墙旁路下的分支DMZ服务器部署方案如下：

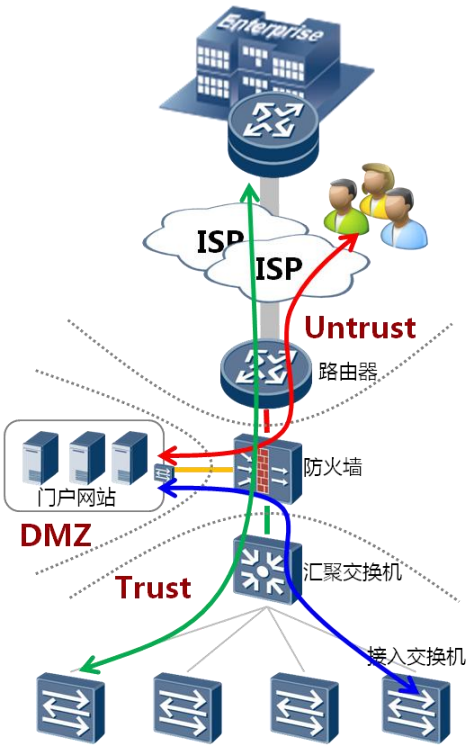


（1）AR路由器接入因特网，并连接到防火墙Untrust区；门户网站通过交换机或直连接入到防火墙DMZ区；分支内网通过汇聚交换机接入到防火墙Trust区.

（2）防火墙工作在混合模式：与Trust、Untrust区透明连接，同时作为网关接入DMZ区服务器。

（3）门户网站配置私网IP，在AR路由器上固定NAT映射到公网IP。

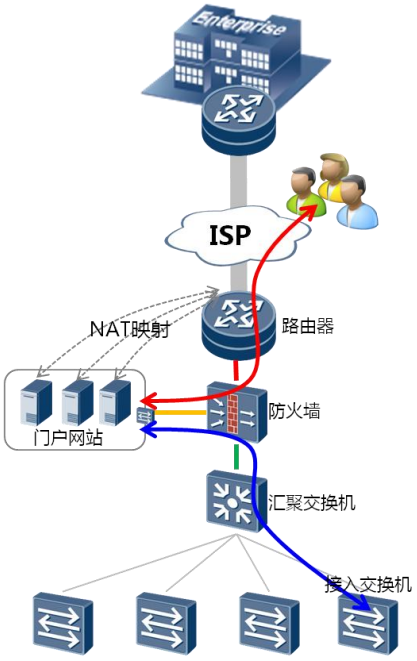
防火墙直路部署



防火墙串联在路由器和汇聚交换机之间，防火墙工作在混合模式，透明接入Trust、Untrust区域，并作为三层网关接入DMZ区。串联方式很好的隔离了分支内部网络、DMZ区和互联网区，并且无需配置策略路由。

采用防火墙直路部署，对于内部有门户网站的大/中型分支，对安全要求比较高，单纯采用AR集成防火墙无法阻止来自因特网的攻击，须采用专业防火墙做安全隔离。

防火墙旁路下的分支DMZ服务器部署方案如下：



（1）AR路由器接入因特网，并连接到防火墙Untrust区；门户网站通过交换机或直连接入到防火墙DMZ区；分支内网通过汇聚交换机接入到防火墙Trust区。

（2）防火墙工作在混合模式：与Trust、Untrust区透明连接，同时作为网关接入DMZ区服务器。

（3）门户网站配置私网IP，在AR路由器上固定NAT映射到公网IP。

2.4.7 NAC 解决方案

在企业网络中，任何一台终端的安全状态（主要是指终端的防病毒能力、补丁级别和系统安全设置）都将直接影响到整个网络的安全。另外，大量非法接入和非授权访问的状况，将导致企业业务系统的破坏，以及关键信息资产的泄漏。从安全角度来分析，目前大部分的企业内部网络中，主要存在如下一些安全问题：

内网安全问题

1、对于感染病毒和木马的终端无法进行控制其访问，只能通过管理手段要求分员工对终端进行杀毒。并且该工作是事后的工作，当一个未知病毒大面积爆发时有可以造成整个网络无法使用，对网络的安全稳定运行造成非常大的影响。

2、各终端不打、漏打系统补丁状况严重，而且没有办法强制安装，导致一旦某台终端感染病毒或恶意代码，则很快就会在内网泛滥。

3、员工安全意识薄弱，员工私自安装不合法软件，或者通过调制解调器、ISDN 拨号设备、ADSL 拨号设备、无线网卡等网络设备非法接入互联网，给网络的安全性等带来了极大的隐患。而企业的安全系统无法这些情况进行检测和控制，难以实施有效的安全策略。

4、企业安全系统无法实时监控系统安全状态，无法对员工网络访问行为、非法外联行为、USB 存储设备使用等行为进行审计并上报安全策略服务器，缺乏事后安全审计的手段。

NAC 方案价值

华为的 NAC 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 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。

1、身份认证和访问控制：NAC 方案可以对接入网络的用户身份进行合法性进行认证，只有合法用户才允许接入，并且不同的角色，不同的用户所能够访问的资源是不同。管理员可以为用户分组，或者定义不同的角色，配置不同的资源，使得特定的用户只能访问授权的特定资源，禁止访问未授权的网络资源。

2、接入安全检查和控制：NAC 方案可以对用户终端的安全性进行检查，只有“健康的、安全的”用户终端方可接入网络。企业网络管理人员可以自定义企业网络安全规则和策略，比如终端必须安装启动防病毒软件、病毒库必须是最新的，终端系统不得安装违规软件，必须安装系统补丁等等。

3、系统修复与升级：如果系统存在安全隐患，华为 NAC 方案提供了系统自动和手动的修复升级功能。支持与 WSUS（Windows Server Update Services）的联动，可自动下载

和升级系统补丁；提供与商业防病毒软件的强联动，触发病毒谱的更新；可自动杀死非法/违规进程等强制安全措施。

4、丰富的扩展特性：华为 NAC 解决方案，还提供行为管理、软件分发、资产管理等等扩展功能。

- 行为管理

  TSM 提供基于终端的员工行为管理功能，目的在于提醒终端用户在使用终端主机时遵守企业制定的行为规范，通过规范员工的行为来提高内网安全管理的能力。

- 软件分发

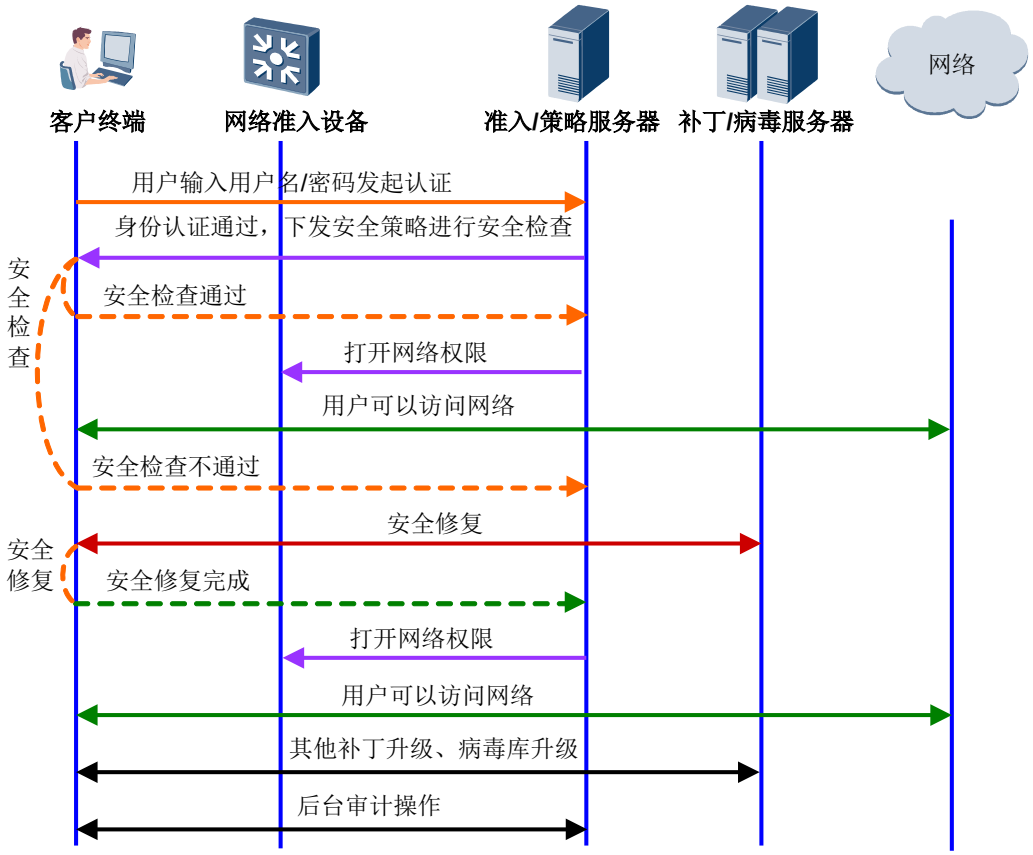
  TSM 提供软件分发功能，将软件手工或按计划自动分发到相应的终端主机上，并支持按部门、按操作系统进行分发。

- 资产管理

TSM 提供资产管理功能，统一管理企业资产，提高效率，降低维护成本，避免员工私自更改企业终端主机的配置，降低资产遗失的风险。

NAC 方案流程

结合终端代理、网络准入设备、准入服务器各个组件，NAC 方案的基本流程所示。



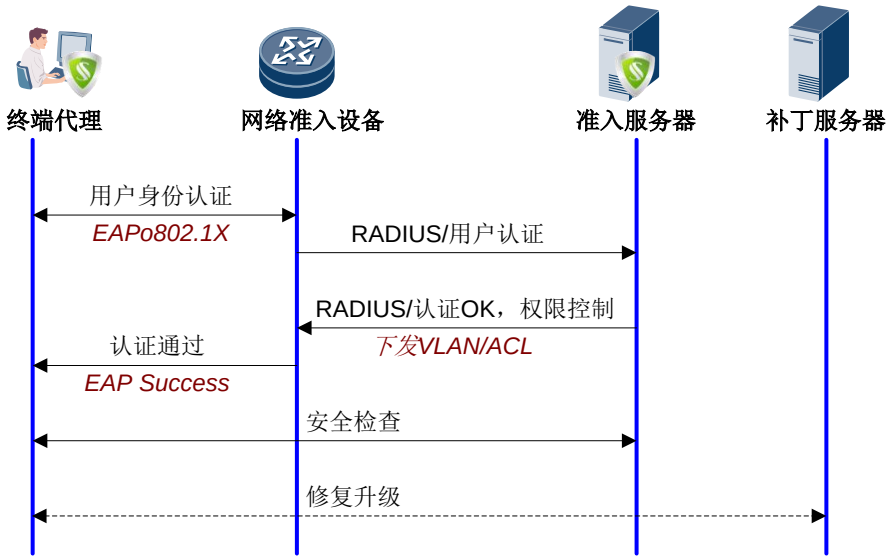
详细流程说明如下：

1. 客户端接入网络，认证前都具有认证前域网络权限，可以根据需要进行终端代理软件安装，补丁安装，杀毒软件安装、升级等操作。
2. PC 客户端安装终端代理软件或 Web Agent 插件，用户输入用户帐号和密码发起身份认证，身份认证通过后，终端代理软件或 Web Agent 插件与准入服务器联动检查终端安全状态。
3. 对合法并安全的用户，身份认证后，准入服务器下发网络权限到网络准入设备，允许该用户访问认证后域网络。
4. 对合法但存在较低安全风险的用户，身份认证后，准入服务器下发网络权限到网络准入设备，允许该用户访问认证后域网络，同时提示终端安全风险。
5. 对合法但严重不安全的用户，身份认证后，准入服务器下发隔离域网络权限到网络准入设备，仅允许该用户访问隔离域网络，用户安全修复后，重新下发网络后域网络权限。
6. 支持用户在线实时安全状态检查，上线用户使用过程中出现严重安全问题，仍会被隔离。
7. 非法用户及未认证用户仅允许访问认证前域网络资源

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。



详细的流程说明如下：

1. 用户终端接入网络，终端代理与网络准入设备通过 EAP 交互帐号和密码信息。
2. 网络准入设备与准入服务器通过 RADIUS 协议，对终端用户身份合法性进行认证。
3. 用户认证通过后，准入服务器通过 RADIUS 协议告知网络准入设备，同时下发用户接入的 VLAN 归属号或对应的 ACL，实现对认证后合法终端用户的访问控制。
4. 网络准入设备通过 EAP Success 消息通知用户终端。
5. 终端代理与准入服务器交互终端系统安全状态信息，对用户终端的进行安全检查。
6. 如果用户终端不安全，终端代理启动系统修复升级工作，与相关服务器（补丁、病毒库等）交互，完成系统的安全修复。

当客户网络由于特殊的情况，不能在底层接入交换机上部署 802.1X 协议时，或者接入交换机下挂 HUB 接入多个用户终端的情况下，标准的基于端口的 802.1X 协议就无法实现对各个终端的单独访问控制。

华为针对上述问题，在交换机、路由器上对标准 802.1X 协议进行了功能增强，实现了基于 MAC 的 802.1X 访问控制，可实现当单端口接入多用户终端时，针对具体单个终端的访问控制。华为的 NAC 方案中同时支持基于端口和基于 MAC 的 802.1X 访问控制，用户网络可以有针对性的选用。

- 基于端口模式：当采用基于端口方式时，只要该端口下的第一个用户认证成功后，其他接入用户无须认证就可使用网络资源。但是当第一个用户下线后，其他用户也会被拒绝使用网络。
- 基于 MAC 模式：当采用基于 MAC 地址方式时，该端口下的所有接入用户均需要单独认证。

在用户终端的访问控制方面，可以通过下发 VLAN 或下发 ACL 方式（也可以两者同时使用）。根据控制方式的不同，802.1X 认证可进一步细分为基于 Guest VLAN 的 802.1X 认证和基于 ACL 的 802.1X 认证。

- 基于 Guest VLAN 的 802.1X 认证

  这是业界最常用的 802.1X 认证方式，用户认证前缺省归属 Guest VLAN，认证通过后准入服务器下发用户认证后的相应角色 VLAN 号，将用户终端从 Guest VLAN 切入到相应角色 VLAN。
- 基于 ACL 的 802.1X 认证

  该方式下，用户终端认证通过后，准入服务器仅下发用户 ACL 实现针对该用户的访问控制。该方式在大用户量情况下，对设备 ACL 规格要求较高。

另外，准入设备首先触发用户采用 802.1X 认证方式，如果用户长时间内没有进行 802.1X 认证，则以用户的 MAC 地址为认证信息，把 MAC 地址作为用户名和密码上送服务器进行认证。此种认证方式被称为 MAC 旁路认证。

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。

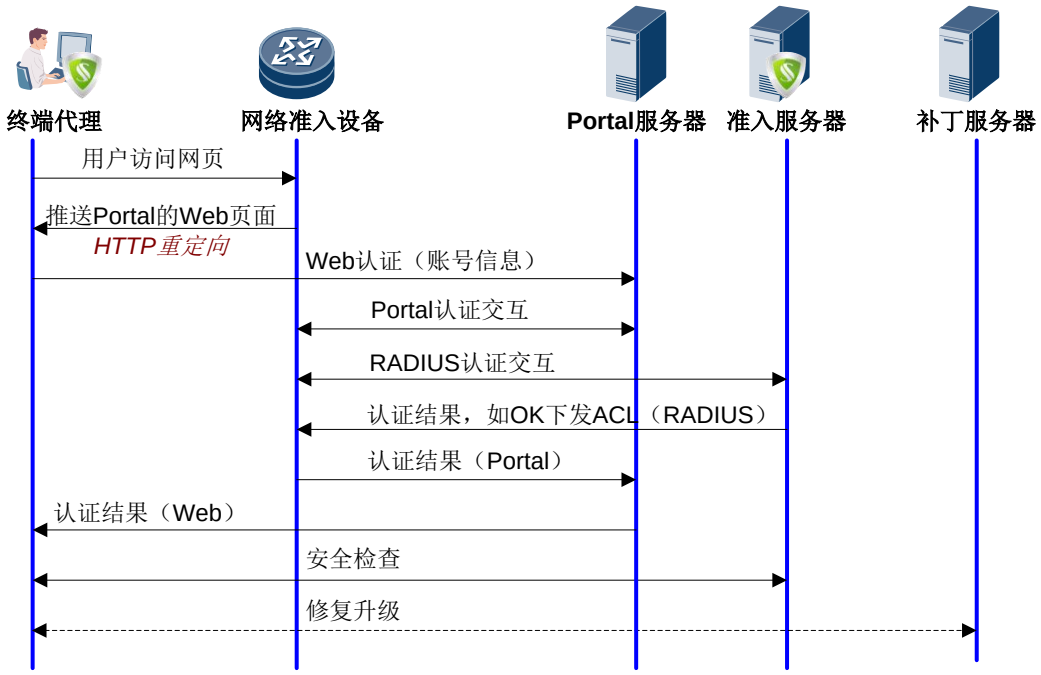
Portal 认证支持 Web 认证且可以无需安装客户端软件，这两个特性使得 Portal 认证对于访客和出差用户具有很好的支持。

说明

Portal 认证方式下，仍旧可以通过下载客户端的方式实现完整的终端准入控制功能特性。

在 Portal 的 Web 认证前，用户首先要访问认证页面，在认证页面输入帐号和密码，然后提交。用户访问认证页面的过程，可以采用主动访问页面和被动访问页面即强推的方式来实现。

Figure 2-1 Portal 认证流程图



详细的流程说明如下：

1、 终端访问任意 Web 服务器（注：如果访问的是某个域名，此域名要是 DNS 服务器可以解析的）。

2. 网络准入设备截获用户 HTTP 请求，如果非 Portal 服务器，通过 HTTP 重定向命令推送 Portal 的 Web 认证页面。

3. 用户终端访问 Portal 服务器 Web 认证页面，输入帐号/密码，提交认证。

4. Portal 服务器与网络准入设备通过 Portal 协议交换用户帐号信息。

5. 网络准入设备通过 RADIUS 协议，向准入服务器（RADIUS 服务器）进行用户认证。

6. 准入服务器进行用户身份认证，并反馈认证结果。如果认证通过，一并下发用户 ACL。

7. 网络准入设备收到 RADIUS 认证结果，通过 Portal 协议告知 Portal 服务器。如果认证成功，放开用户上网权限，并启动 ACL 实现该用户的网络访问控制。
8. Portal 服务器向用户终端通过 HTTP 通知认证结果。
9. 用户终端下载安装 ActiveX 控件（或安装了客户端代理软件），认证通过后，终端代理将与准入服务器进行安全状态信息交互，实现对终端用户的安全性检查。
10. 如果用户终端不安全，终端代理启动系统修复升级工作，与相关服务器（补丁、病毒库等）交互，完成系统的安全修复。

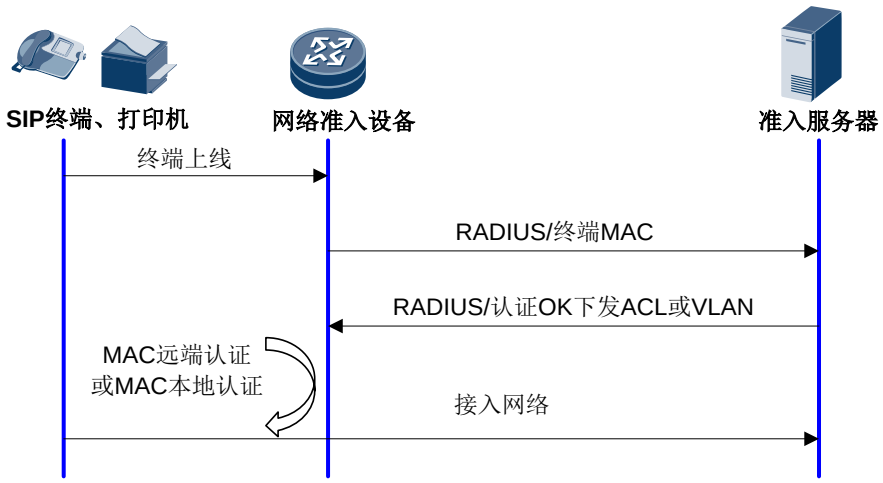
MAC 认证

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。

对于用户的 MAC 认证，即可以是本地认证，也可以是远端 RADIUS 服务器认证。如果采用 RADIUS 认证，用户的访问权限由 RADIUS 服务器下发的 ACL 或 VLAN 来控制。

Figure 2-2 MAC 认证流程图



MAC 认证的详细流程如下：

1、 设备上线，网络准入设备自动提取终端 MAC 地址。

2. 网络准入设备对终端设备 MAC 地址进行认证：

- 如果采用 RADIUS 认证，网络准入设备将终端设备 MAC 地址作为帐号和密码，通过 RADIUS 协议送准入服务器认证。
- 如果采用本地认证，网络准入设备在本地配置的 MAC 认证表中对终端设备 MAC 地址进行认证。

3. 认证通过后，打开该终端设备的上网权限。如果 RADIUS 认证，采用 RADIUS 下发的 ACL 或 VLAN 对终端设备进行权限控制。

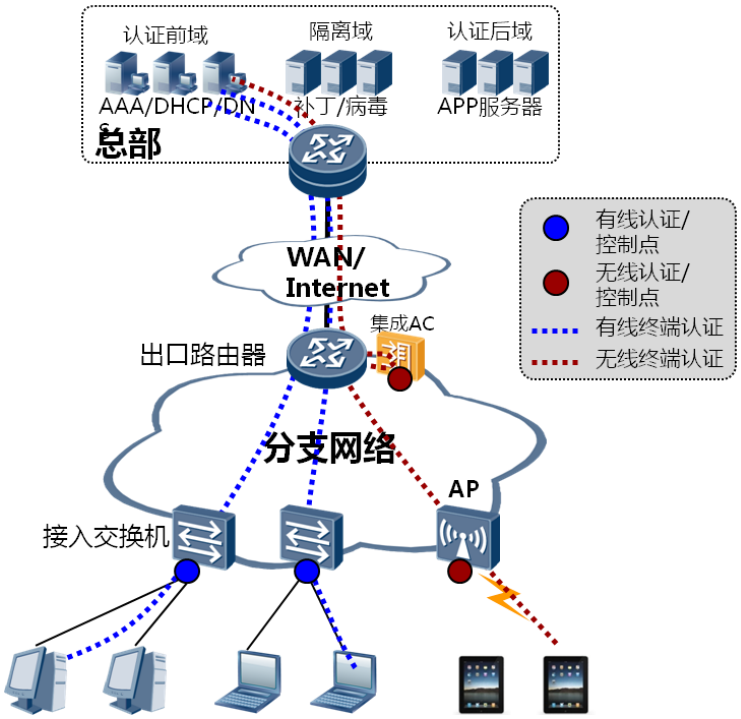
三种认证方式比较

802.1X 认证、Portal 认证和 MAC 认证的优劣势比较所示。

对比项	802.1X 认证	Portal 认证	MAC 认证
客户端需求	必须	Portal 需要，web 强推不需要	不需要
优点	部署在接入层时，直接控制网络接入信息口的通断，安全性高	部署灵活	无需安装客户端
缺点	部署不灵活	安全性不高	管理复杂，需登记 MAC 地址
适合场景	新建网络，用户集中，信息安全要求严格的场景	认证方式灵活，适用于用户分散，无线场景	适用于 SIP 终端，打印机，传真机等哑终端接入认证的场景

802.1X 认证部署规划建议

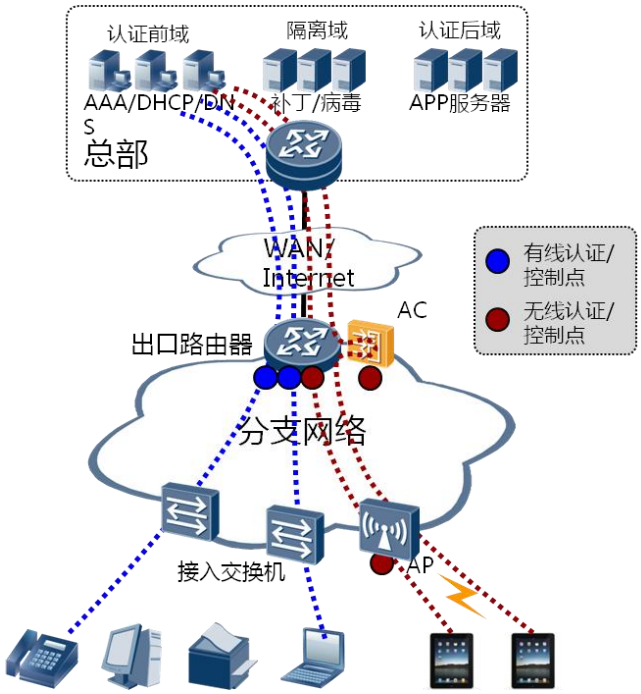
802.1X 认证适用于各种规模的分支场景，特别是用户对安全控制要求高的场景。可选择在接入层部署 802.1X＋MAC 混合认证方式。



接入交换机启用 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。服务器系统为 TSM 服务器组件，基于用户组进行用户管理和权限控制。方案价值是控制点离用户最近，内网得到最大安全保障，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。

Portal 认证部署规划建议

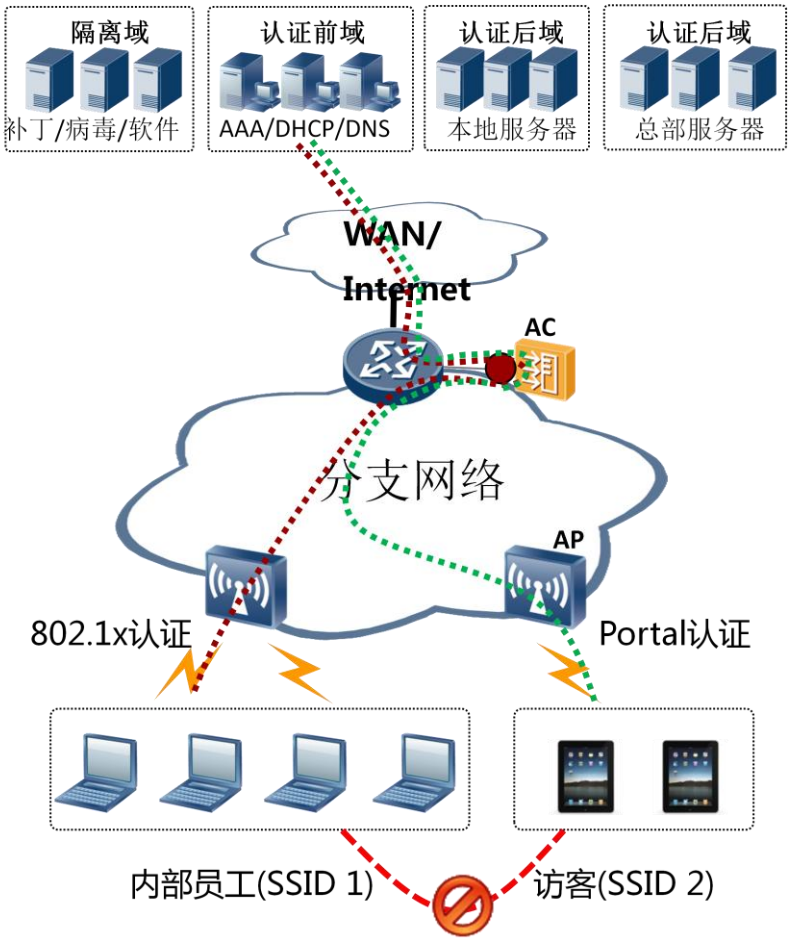
Portal 认证适用于微小型分支网络，对安全要求不高的场景，在出口路由器部署 Portal ＋MAC 混合认证，适用于接入交换机不支持 802.1x 认证的旧网改造场景。



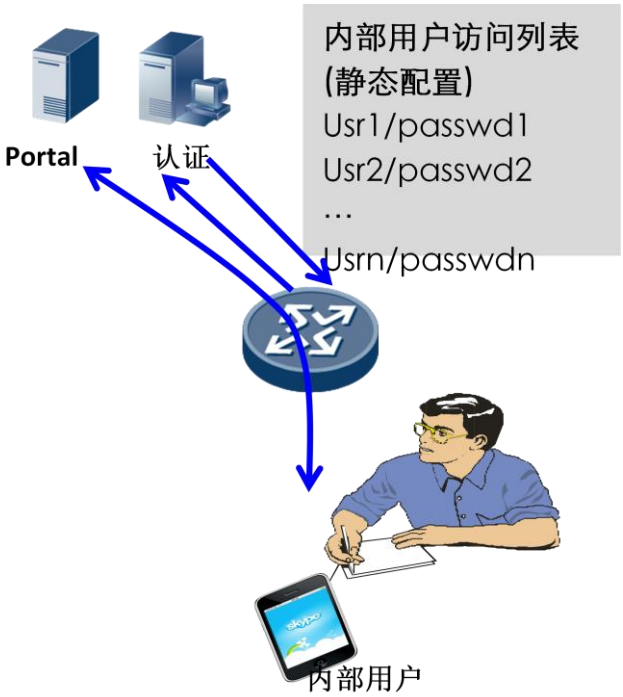
出口路由器启用 Portal＋MAC 自适应混合认证，有线用户做 Portal 认证，IP 电话、打印机等哑终端做 MAC 认证。如果需要无线接入，可采用具有内置 AC 功能的出口路由器，无线终端也通过 Portal 认证接入。出口路由器内置 Portal 服务器功能，认证系统统一部署在总部。方案价值是 NAC 认证点上移到出口路由器，控制点单一，方便管理维护。AR 路由器内置 AC 功能，有线无线一体化认证。

WLAN 部署规划建议

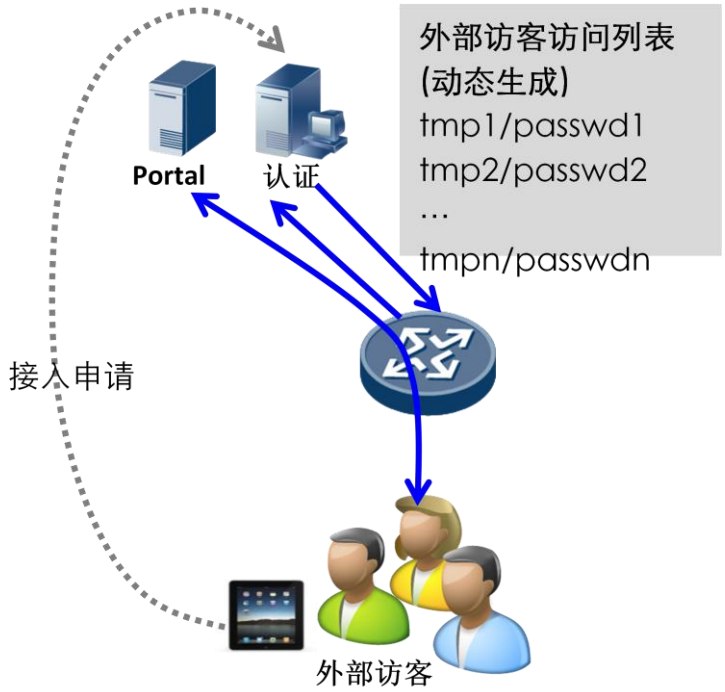
WLAN 接入认证分两种情况，外部访客采用 Portal 认证，免装客户端，方便接入；内部员工采用 802.1x 认证，更安全。



对访客只开放 Internet 和 DMZ 资源，禁止访问认证后域的企业内部资源；内部员工根据需要办公开放资源。内部员工与访客分别接入不同 SSID，并禁止两者互访，提升网络安全。



内部用户认证流程：企业内部员工的账号/密码已事先配置在认证服务器中。员工选择接入员工专用 SSID，访问任何网页时，在 Portal 服务器推送的页面上填入自己的账号/密码，认证/授权后即可上网。员工根据授权服务器的授权，访问相应的内部服务。

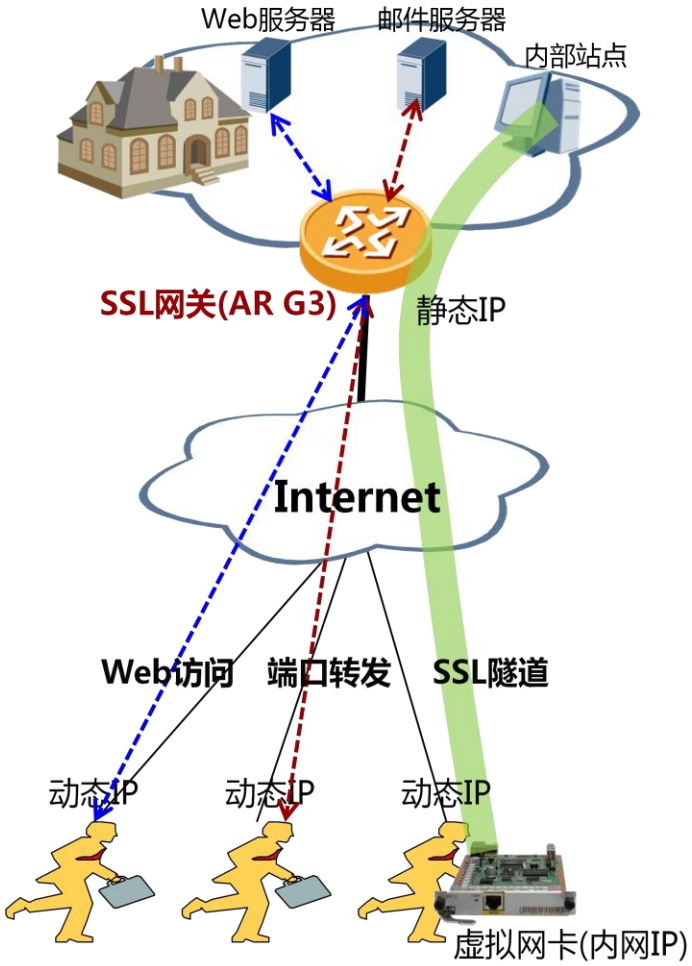


外部访客认证流程：外部访客携带 pad 或智能手机等终端接入分支无线网，上网前需先申请。申请有几种常见方式：WEB 页面填入手机号，手机短信接收密码；自助机上扫

描二代身份证，获取密码；以微博/QQ 账号/密码接入 Wifi。外部访客只开放 Internet/DMZ 服务器访问权限。

远程用户/合作伙伴接入部署规划建议

适于出差员工、合作伙伴等个人用户远程接入场景，一般采用 SSL VPN 方式接入，无需安装客户端，方便接入。

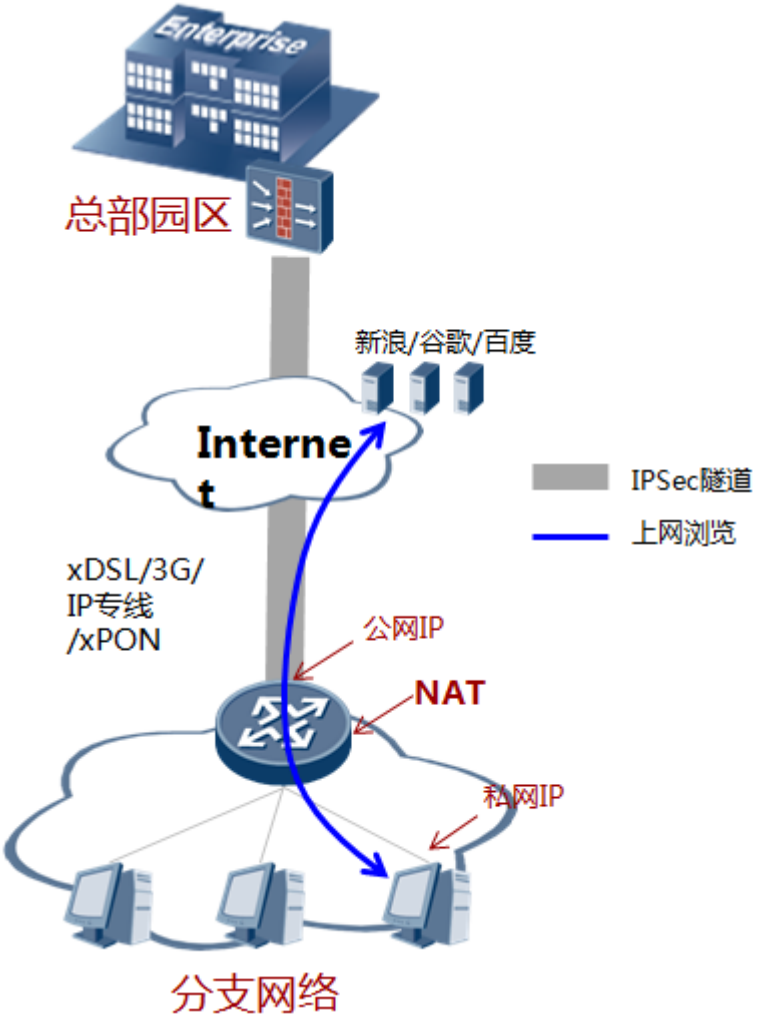


微/小型分支，远程接入用户在几人以内，出口路由器 AR1220 兼做 VPN 网关。大/中型分支，远程接入用户一般在几十到一百人，出口路由器 AR22/32 作为 VPN 网关。远程用户通过 VPN 接入后，可直接到认证服务器进行认证。方案价值是 AR 路由器内置 SSL VPN 功能，节省投资。内部用户、合作伙伴一体化管理，方便运维。

3 分支网络业务设计

3.1 Internet 访问

3.1.1 分支单链路接入 Internet



分支单链路接入 Internet 接入特点：

- 适用场景

  分支机构希望能从本地直接上因特网，并且对分支/总部互联可靠性/安全性要求不高

- 接入方式

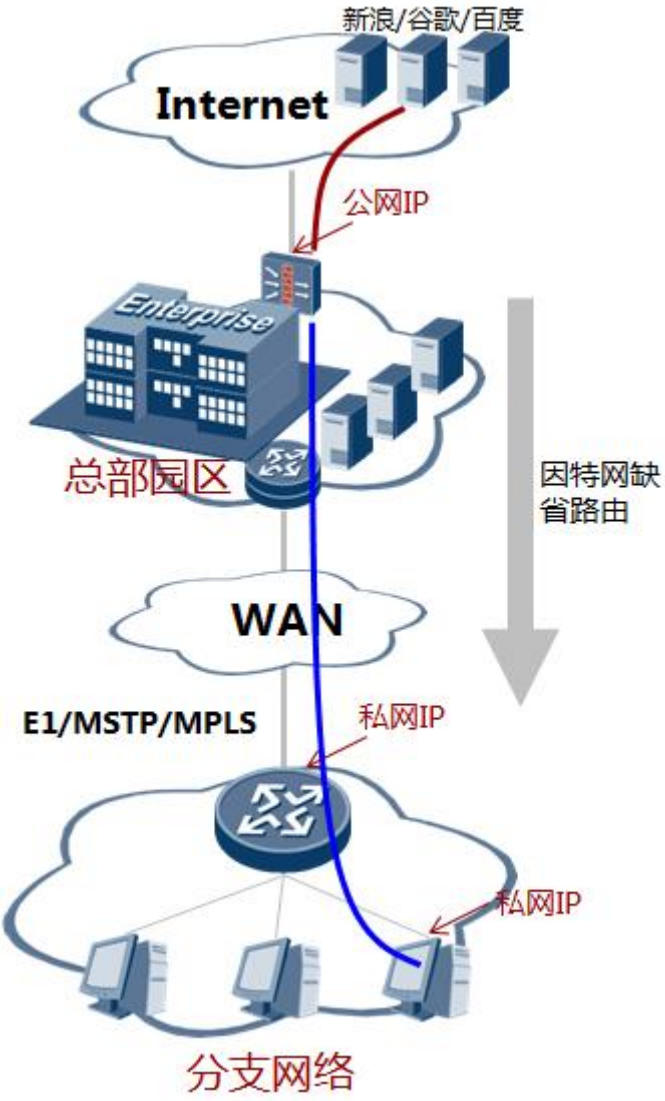
xDSL/3G 拨号：分支出口路由器得到公网或私网 IP 地址。对于私网地址，不支持出差用户/合作伙伴远程接入。费用低廉。

因特网专线：有以太专线和 xPON 专线两种方式。灵活带宽的高品质接入。运营商分配一个或多个公网地址，方便本地服务器 NAT 固定映射，支持访客/出差用户/合作伙伴远程接入。

- 方案特点

  各分支自行解决上网问题，灵活选择接入方式。分支与总部隧道互联，无需租用 WAN 专线，节省投资。

3.1.2 分支通过总部接入 Internet



分支通过总部接入 Internet 特点：

- 适用场景

分支/总部间互联可靠性要求高，往往采用 WAN 专线互联。此种场景下，上网流量只能绕行总部，总部可以部署防火墙和上网行为管理。

- 接入方式

  分支租用专线与总部之间通过 WAN 连接，包括 E1/MSTP/MPLS 专线。

  总部通过专线接入因特网，部署防火墙和上网行为管理，保障网络安全。

- 方案价值

  企业所有上网流量走统一出口，节省上网费用。

  统一出口，便于集中部署防火墙和上网行为集中管理，网络更安全。

  上网流量与分支流量公用 WAN 专线，需考虑部署 Qos 策略，防止低优先级的上网业务占用过多带宽

3.2 语音

3.2.1 企业语音通信业务面临的挑战

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。

然后，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，例如一号通业务，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。

3.2.2 企业语音通信业务的挑战目标

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 网络相媲美的语音通信系统。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。

3.2.3 IP 语音系统设计的基本原则

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。

企业语音用户拔打外线出局选择原则

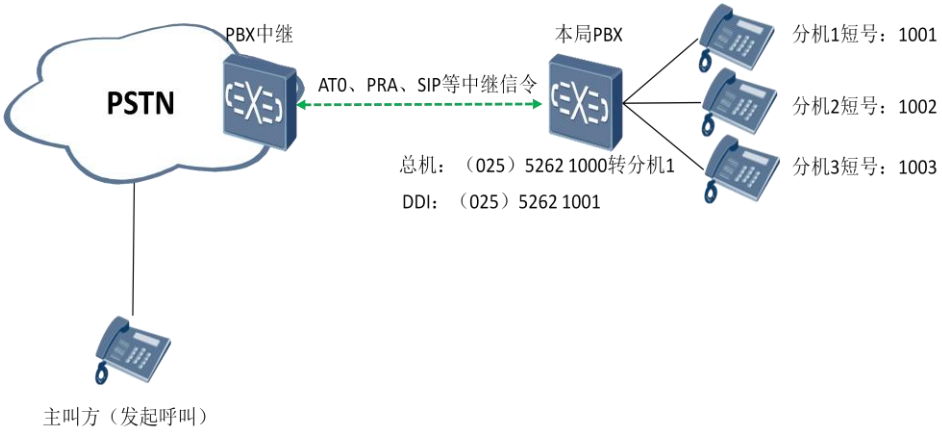
- 企业是外贸型企业，企业的通信主要是对外通信，则建议企业向运营商申请的出局收敛比为 1:2 或者 1:1.5。
- 企业是生产型/研发型企业，企业的通信主要是内部通信，则建议企业向运营商申请的出局收敛比为 1:4~1:10。

企业如果是大型企业，同时企业的语音用户数量非常多并且每个用户都需要运营商号码的情况下，则建议企业部署企业总机+内部分机的方式或者企业向运营商申请 Centrex 组网。

3.2.4 语音基础知识

PBX

PBX：Private Branch Exchange，俗称程控交换机，主要功能是完成企业内部之间以及与PSTN 的电话交换。PBX 可以分为传统 TDM-PBX 和 IP-PBX。TDM-PBX 只能处理语音模拟信号，仅提供语音业务，无法处理视频及基于 IP 应用的各类业务。IP-PBX 在 TDM-PBX 的基础上，增加对语音数字信号、IP 应用的全面支持。



分支机构内每部电话都有一个短号和长号，内部通话直接使用短号拨打。如分机 1 直接拨打 1002 可以跟分机 2 通话。长号可以采用总机/分机方式或者 DDI 方式。

- 总机/分机方式

  1 个 PBX 交换机绑定 1 个或多个公网号码，如（025）5262 1000

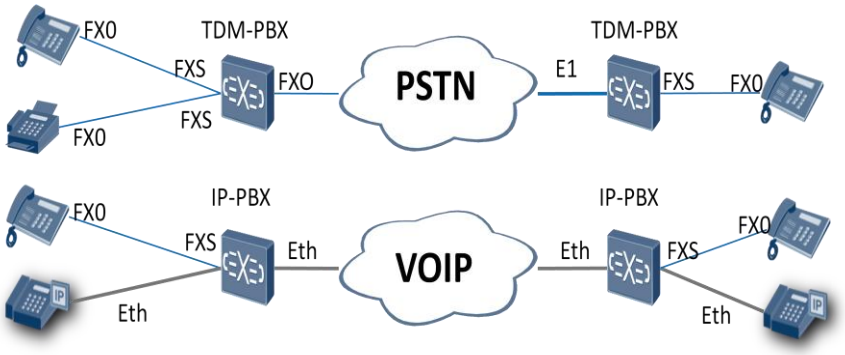
  通过总机（人工或者自动）将来电转接到分机，如分机 1001、1002

- DDI 方式

  DDI:Direct Dialing In，直拨入业务，在此业务中，DDI 号码的呼叫直接到达分机，或者通过 ACD 到达分机组，无需企业的操作员的介入。通过固话运营商申请一组 DDI 号码，话机长号跟短号一一对应，如分机 1 短号为 1001，长号为（025）5262 1001。

语音接口

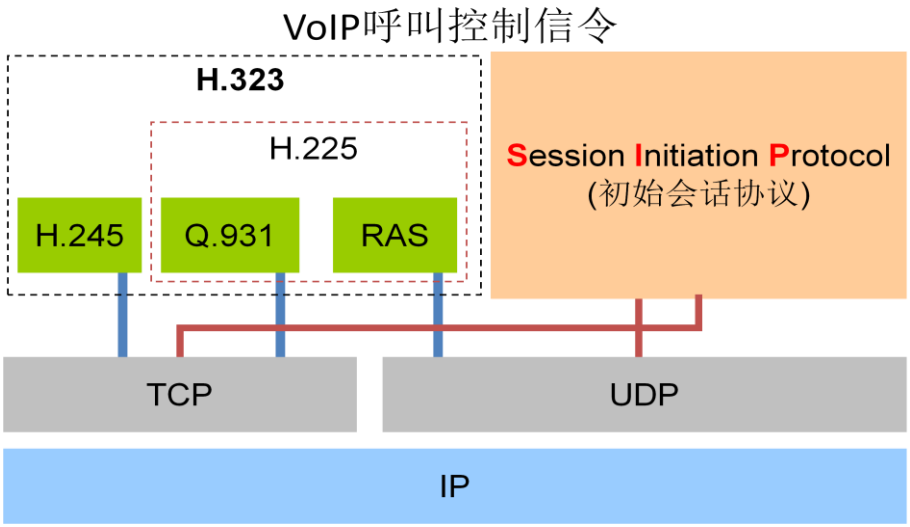
- 模拟接口：FXS（Foreign exchange station）外部交换站，简称 S 口。是 PBX 上用来连接模拟话机或传真机的接口，用于传送拨号音，电池电流以及响铃电压。FXO（Foreign exchange office）外部交换局，简称 O 口。它是模拟电话或者传真机上的接口，也是 PBX 接入 PSTN 的一种接口，FXO 最大支持 1 路语音信道。FXO 和 FXS 总是成对出现的，类似插头和插座的关系。
- 数字接口：E1VI/T1VI（E1/T1 Voice Interface），PBX 出本端交换局的中继接口，欧洲和我国主要使用 E1 标准，北美、日本使用 T1 标准。E1 通信链路为 2M，最大支持 30 路语音信道。常用 E1 接口承载 R2、PRA 等语音中继信令。以太接口，在 IP 网络融合语音通信后（VOIP），出口路由器兼容 PBX 功能，以太接口同时承载数据和语音信息，语音中继信令一般为 SIP 中继或者 H.323 中继。



VOIP 信令

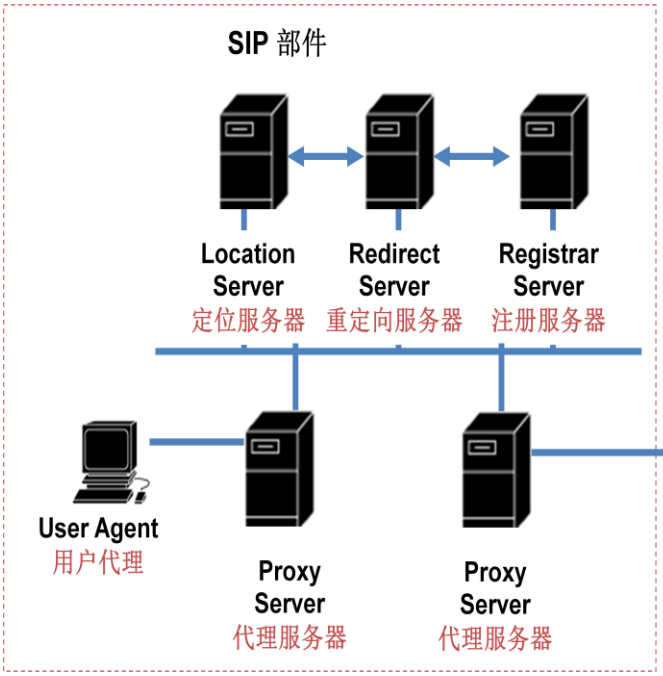
H.323：ITU-T 提出的一个建议书，由一组协议构成，包括信令控制协议 H.225、媒体控制协议 H.245 等等。H.323 并不是为 IP 电话专门提出的，因而它涉及的范围要远比 IP 电话宽。

SIP：另一套 IP 电话的体系结构，由 IETF 提出，是一个与 H.323 并行的协议。目前 SIP 正因其简单、轻量级、易扩展等特点成为广大厂商追逐的新标准，SIP 已成大势所趋。



SIP 简介

SIP（Session Initiation Protocal）称为会话初始协议，是由 IETF（Internet Engineering Task Force）组织于 1999 年提出的，是一个在基于 IP 网络中，特别是在 Internet 这样一种结构的网络环境中，实现实时通信应用的一种信令协议。而所谓的会话（Session），就是指用户之间的数据交换。在基于 SIP 的应用中，每一个会话可以是各种不同类型的内容，可以是普通的文本数据，也可以是经过数字化处理的音频、视频数据，还可以是诸如游戏等应用的数据，应用具有巨大的灵活性。



- 用户代理：又称为 SIP 终端，是 SIP 系统中的最终用户，在 RFC3261 中将它们定义为一个应用。根据它们在会话中扮演的角色的不同，又可分为用户代理客户机（UAC）和用户代理服务器（UAS）两种。其中前者用于发起呼叫请求，后者用于响应呼叫请求。
- 代理服务器：是一个中间元素，它既是一个客户机又是一个服务器，具有解析名字的能力，能够代理前面的用户向下一跳服务器发出呼叫请求。然后服务器决定下一跳的地址。重定向服务器（Redirect Server）：是一个规划 SIP 呼叫路径的服务器，在获得了下一跳的地址后，立刻告诉前面的用户，让该用户直接向下一跳地址发出请求而自己则退出对这个呼叫的控制。
- 注册服务器：用来完成对 UAS 的登录，在 SIP 系统的网元中，所有 UAS 都要在某个登录服务器中登录，以便 UAC 通过服务器能找到它们。
- 重定向服务器：重定向服务器不会自己提出(issue)任何 SIP 请求；接收 SIP 请求后，把请求中的原地址映射成零个或多个新地址，返回给客户端,由用户代理去进行用户定位的所有尝试。
- 定位服务器：提供位置查询服务，主要是由代理服务器或重定向服务器用来查询被叫的可能的地址信息。

终端类型

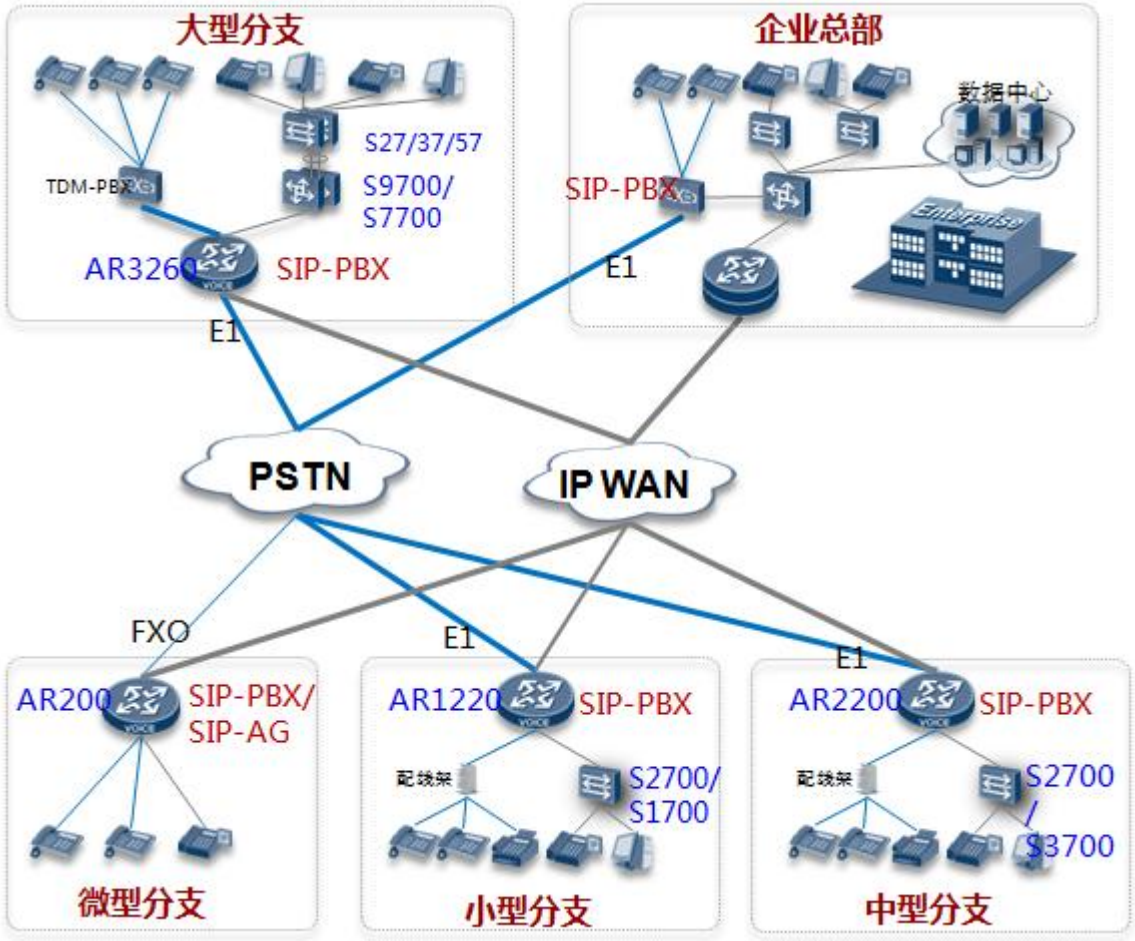
- 模拟电话：模拟电话采用 RJ11 接口接入模拟线路，通用性强，价格便宜，但是存在功能少，接续慢、同时接入的话路有限的缺点。
- IP 电话：相对于模拟语音用户的接入，IP 语音用户具有安装快速，操作简单，统一布线等特点。IP 电话的接入，企业的 IP 网络布线到哪，IP 电话就可以直接通过企业的 IP 网络进行接入，可以通过企业的统一 DHCP Server 进行 IP 电话的地址分配。IP 电话自身具备对信令流及媒体流的 QoS 设置，从而保证了 IP 电话在企业 IP 网络中语音流量的优先处理，提高了 IP 电话在 IP 网络中的服务质量。IP 电话的网线如

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

- PC 软终端：企业通过在员工的 PC 上安装 SIP 软终端，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，可实现号码随人走，不受工作地点的限制。SIP 软终端安装在企业员工的办公 PC 上，企业员工的 PC 通过企业内部的 LAN 网络连接到企业的 Intranet 中，同时 SIP 软终端的用户帐号注册到企业的 SIP 服务器，完成企业员工的语音通信需求。SIP 软终端的 QoS 保证，由于 PC 发生的报文没有携带优先级， SIP 软终端的 QoS 保证由企业的 IP 承载网络进行保证，通过识别 SIP 报文进行优先级添加，从而保证 SIP 软终端的语音用户质量。企业出差员工通过专网 VPN，将安装在 PC 上的 SIP 软终端接入到企业的内部网络，从而实现企业出差员工与公司员工的语音通信。
- 传真机：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。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。

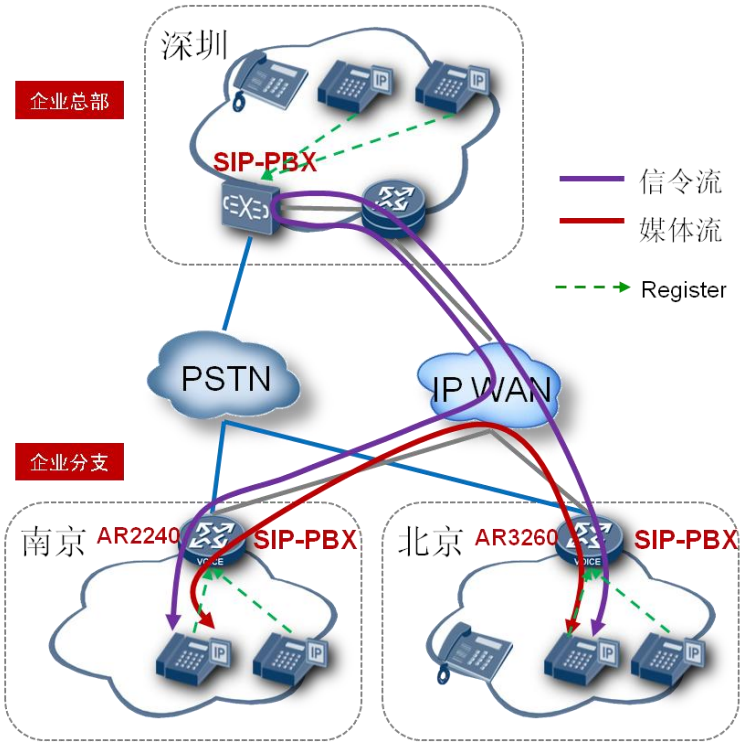
3.2.5 分支语音方案

网络拓扑



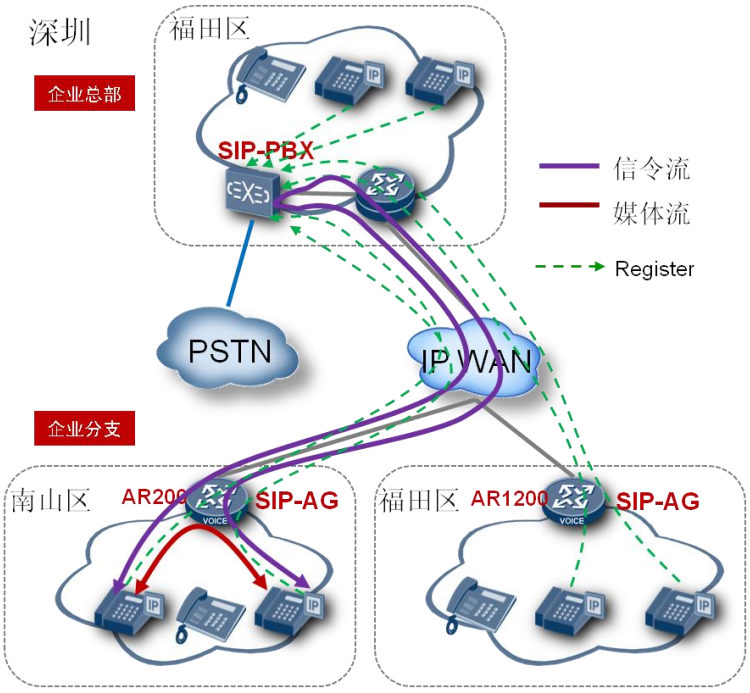
- 大、中、小、微型分支出口 AR 均部署为 SIP-PBX 模式，本地管理语音通话业务。分支跟总部、其他分支通话，统一出局到总部进行语音信令路由处理。
- 微型分支可以根据客户需要部署为 SIP-AG 模式。AG 模式下，则接受总部 PBX 的呼叫控制。AG 模式内置 BEST 功能，可实现总部 PBX 不可达情况下的本地通话功能。
- 本身具有 TDM-PBX 的分支机构，AR 通过 CE1 板卡将 TDM-PBX 接入，保留客户原有投资。通过 LAN 扩展 IP 话机接入。
- 所有分支机构和、总部都通过 FXO（1 路语音在线）、E1（30 路语音在线） 接口接入到本地 PSTN 网络，并作为分支长途互通的备份。

分布式呼叫控制部署



- 分支（含总部）均部署为 SIP-PBX 模式，并且本地语音用户注册到本地 PBX 上。
- 总部 PBX 为各分支互通提供呼叫路由，总部与各分支之间构成分级呼叫路由。
- 分支内拨打直接在本地 PBX 完成呼叫路由查找。分支间拨打，需出局到总部 PBX 上进行呼叫路由查找。
- 分支人数较多规模较大，并且分支和总部比较分散，不在同一城市时推荐使用分布式呼叫控制。

集中式呼叫控制部署



- 分支部署为 SIP-AG 模式，语音用户注册到总部 PBX 上，并为分支提供语音呼叫控制服务。
- 分支内部互拨，呼叫信令流需到总部 PBX 处理，媒体流本地转发。
- AR 部署 SIP-AG 模式，不支持接入 PSTN，拨打 PSTN 用户需由总部的 PSTN 出口。
- 微、小型分支跟总部在同一城市，并且分支与总部间只有基本语音业务时推荐采用 SIP-AG 部署模式。

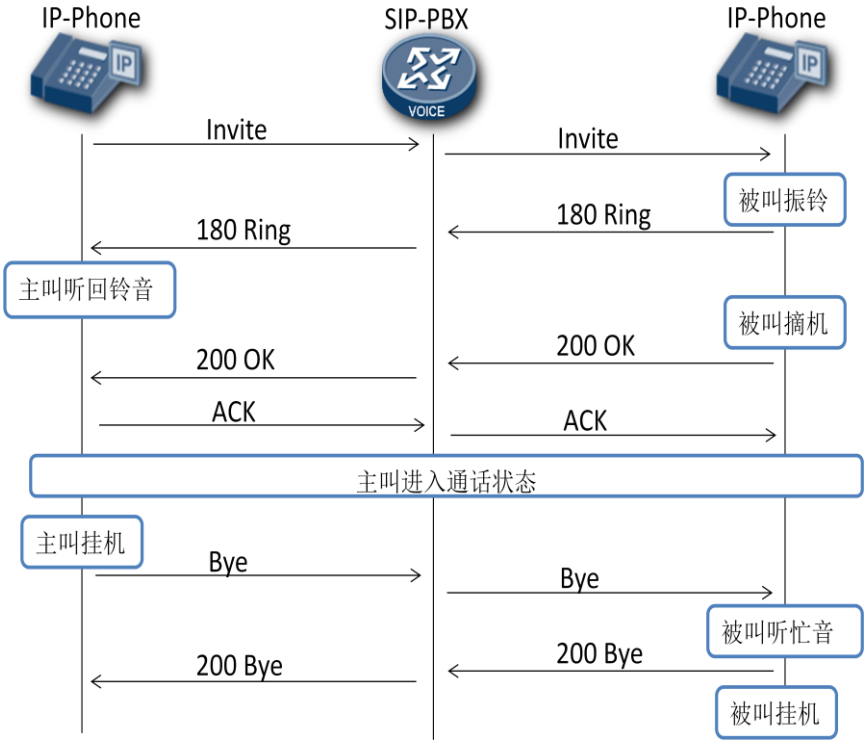
语音控制部署技术比较

比较项	集中式	分布式
AR 部署模式	SIP-AG	SIP-PBX
用户注册	注册到总部 PBX 上	注册到本地 PBX 上
号码规划	总部统一规划	总部、分支分开规划
本地互拨	总部 PBX 呼叫控制	本地 PBX 呼叫控制
分支互拨	总部 PBX 呼叫控制	总部 PBX 呼叫控制
PSTN 互拨	只能从总部 PSTN 出口	本地 PSTN 出口
分支大小	微、小型分支	微、小、中、大型分支
分支语音业务	不支持 IVR、电话会议等业务	PBX 模式比 AG 模式支持更多的语音功能，支持 IVR、电话会议等业务
适用场景		

语音控制部署模型选择

因素	说明
企业各分支机构与企业总部之间的区域位置关系	若分支机构与总部之间在行政区域是同一个区域（企业分支与企业总部的 PSTN 区号相同），建议使用总部集中式呼叫处理，企业所有语音用户注册到总部，通过总部进行企业内员工语音互通。同时企业出局都通过企业总部进行出局呼叫。
	如果企业的分支与总部不属于同一区域，企业分支与总部之间是通过企业 Intranet 连接，建议使用分布式呼叫处理，各分支处理本地呼叫及本地出局。
企业分支机构与企业总部之间人员分布及呼叫流量	企业分支机构人员较少，语音通信量较少，则建议部署集中式呼叫控制，减少企业分支机构的数据配置和维护管理工作。
	如企业分支与企业总部之间的员工数量相当，建议使用分布式呼叫处理，以减少跨企业分支之间的带宽消耗。
企业分支机构与企业总部之间语音业务部署	如果在总部集中部署语音增值业务，则企业各分支为了减少设备的部署，建议企业采用集中式呼叫控制。
	如企业分支需要实现与企业总部同样的增值业务控制能力，则建议企业采用分布式呼叫控制。
企业分支机构与企业总部之间的带宽及 QoS 保障	企业与总部之间的通信带宽如果可以支持语音的带宽要求及 QoS 保障，则建议企业采用集中式呼叫控制。
	企业分支与总部之间的通信带宽及QoS保障不足以支持企业分支与总部之间的语音通信，为了节省企业分支与企业总部之间的带宽，则建议企业采用分布式呼叫控制。

PBX 模式分支内部 IP 话机互拨流程



1、 主叫向 PBX 发起 INVITE 呼叫，携带被叫号码。

2、 PBX 找到被叫，并向被叫发起 INVITE 呼叫。

3、 被叫振铃，并向 PBX 回复 INVITE-180 响应。

4、 PBX 将被叫的 INVITE-180 响应转给主叫，主叫听回铃音。

5、 被叫摘机，向 PBX 发送 INVITE-200 响应。

6、 PBX 将被叫的 INVITE-200 响应转给主叫。

7、 主叫向 PBX 回复 ACK。

8、 PBX 将 ACK 转给被叫。

9、 主叫被叫进入通话态。

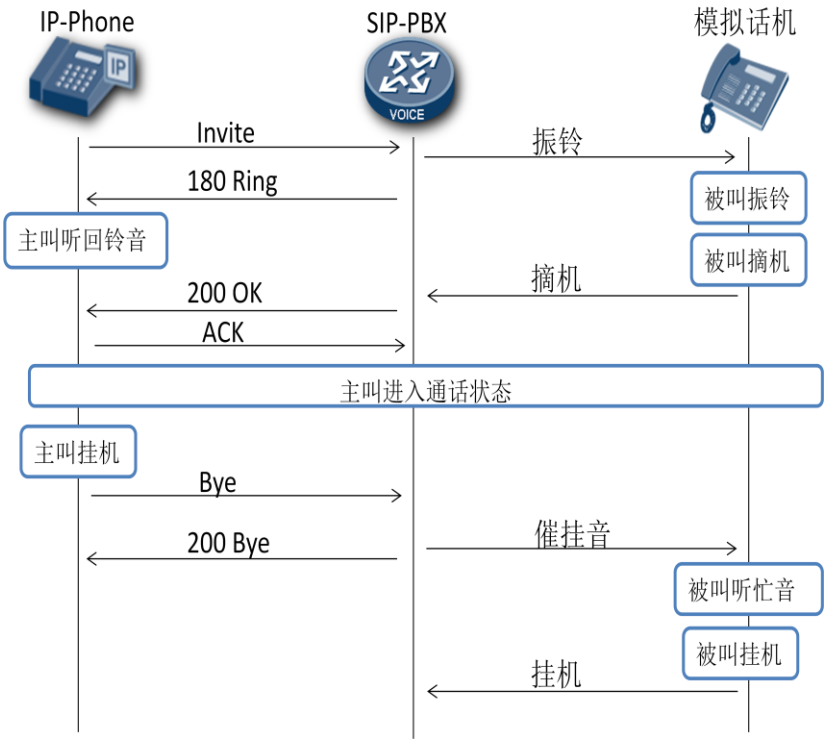
10、 主叫挂机，向 PBX 发送 BYE。

11、 PBX 向被叫转发 BYE，被叫侧听忙音。

12、 被叫向 PBX 回复 Bye-200。

13、 PBX 向主叫转发 Bye-200。

PBX 模式分支内部 IP 话机拨打模拟话机流程



1、 主叫向 PBX 发起 INVITE 呼叫，携带被叫号码。

2、 PBX 接收到 SIP 终端发来的 INVITE 消息，对被叫号码做号码和路由分析，发现是内部呼叫，于是指示被叫 POTS 振铃。

3、 被叫摘机后呼叫建立，PBX 给终端回 200 接受呼叫。

4、 主叫向 PBX 回复 ACK。

5、 主叫被叫进入通话态。

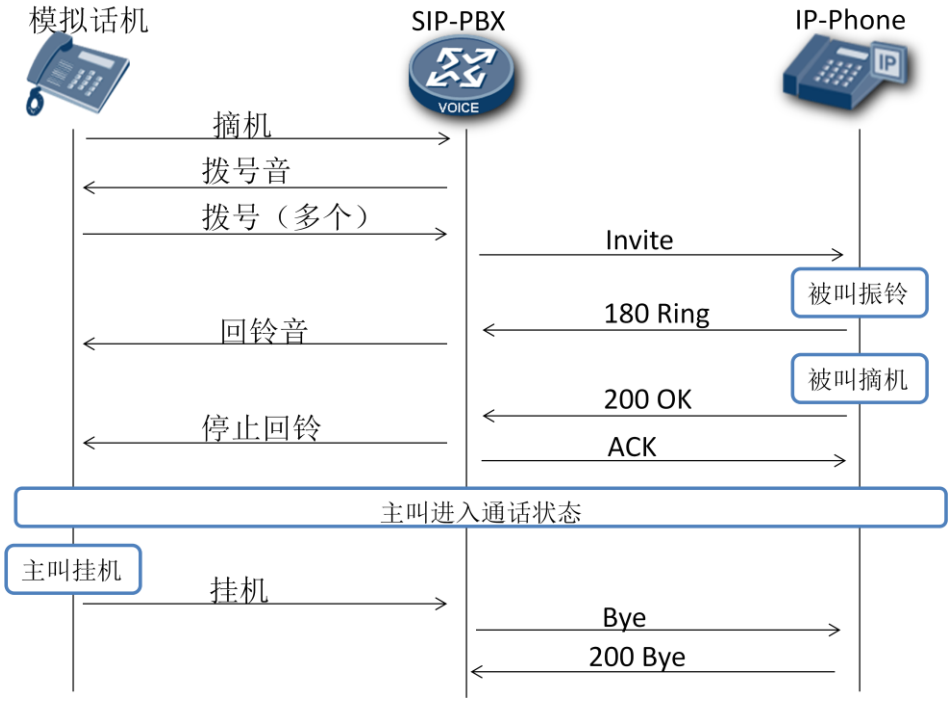
6、 主叫挂机，向 PBX 发送 BYE。

7、 被叫侧听忙音。

8、 PBX 向主叫转发 BYE-200。

9、 被叫挂机，本次通话结束。

PBX 模式分支内部模拟话机拨打 IP 话机流程



1、 主叫摘机，听 PBX 播放拨号音。

2、 主叫拨号，PBX 收齐号码后根据配置分析出该呼叫为本地呼叫，并向被叫发起 INVITE 呼叫。

3、 被叫振铃，并向 PBX 回复 INVITE-180 响应。

4、 PBX 向主叫播放回铃音。

5、 被叫摘机，向 PBX 发送 INVITE-200 响应。

6、 PBX 通知主叫停止回铃音。

7、 PBX 将 ACK 转给被叫。

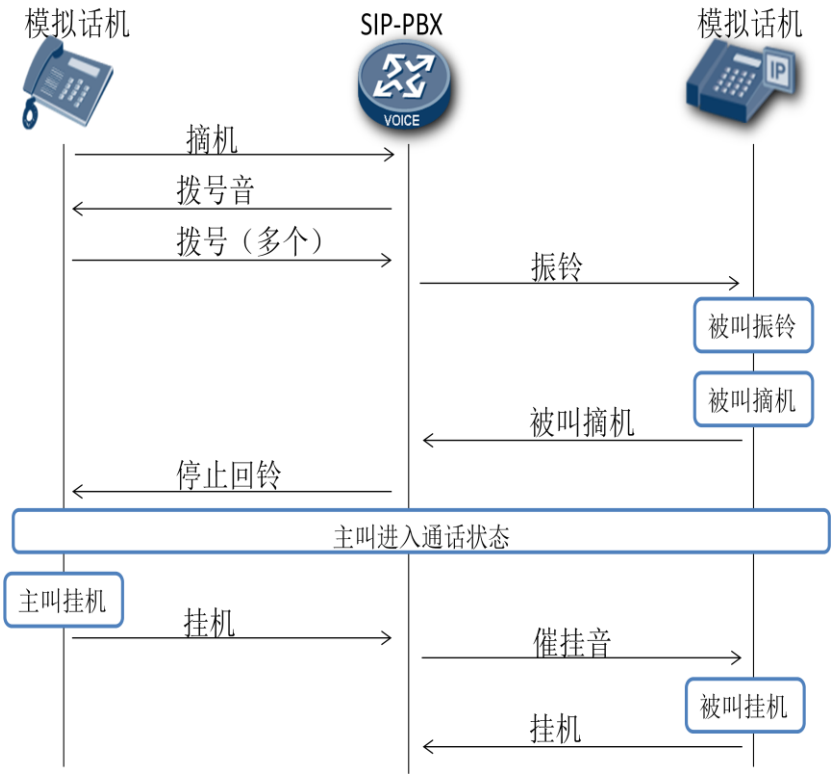
8、 主叫被叫进入通话态。

9、 主叫挂机。

10、 PBX 向被叫发送 BYE。

11、 被叫回应 BYE-200。

PBX 模式分支内部模拟话机互拨流程



1、 主叫摘机，PBX 给用户 A 放拨号音。

2、 主叫拨打用户 B 的号码，PBX 收到第一个号码后，停拨号音，同时进行号码分析。

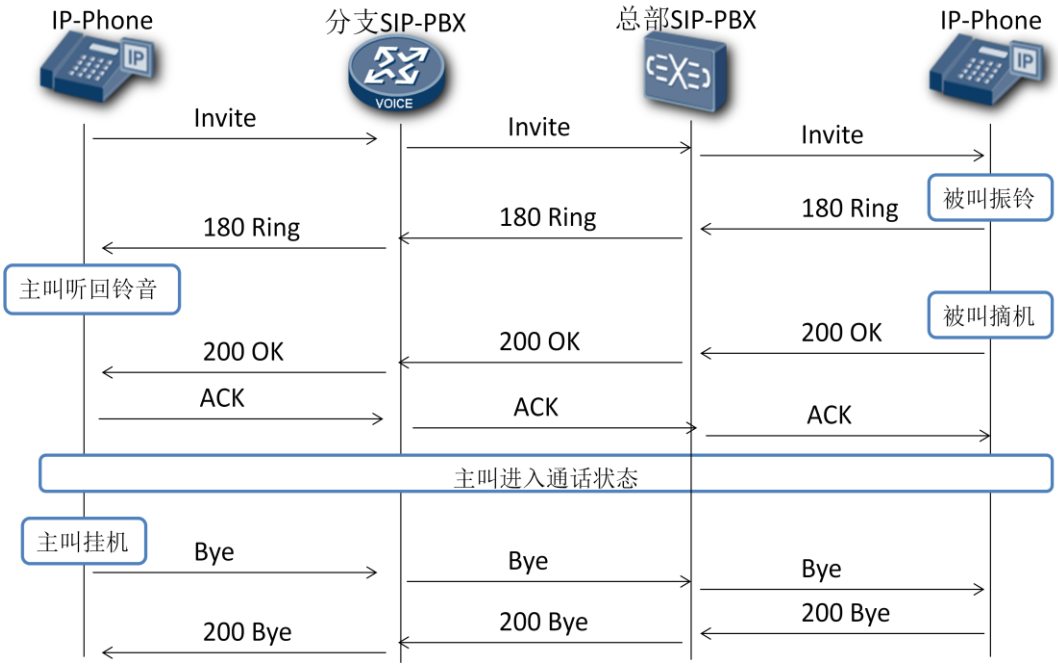
3、 PBX 定位到被叫用户 B 后，给用户 B 发送振铃，如果需要下发主叫号码，则先下发初始振铃，然后发送主叫号码，用户 B 则能看到主叫用户 A 的号码。

4、 主叫听回铃音。

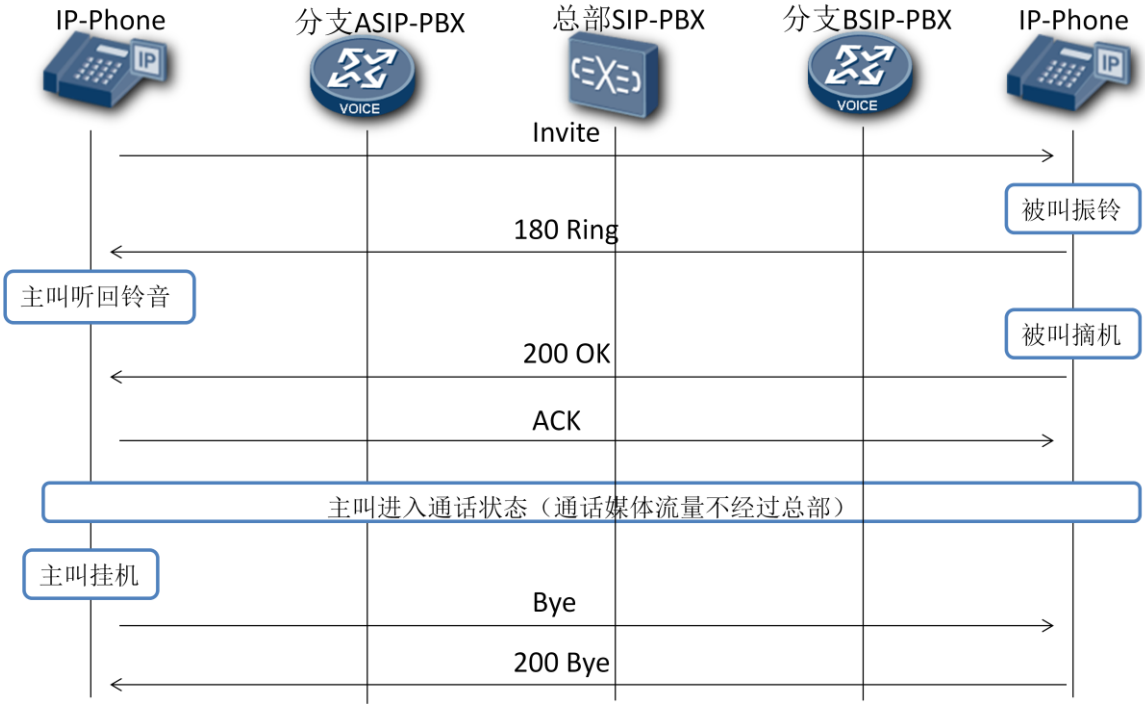
5、 主叫挂机，PBX 给用户 B 放忙音。

6、 被叫挂机，通话结束。

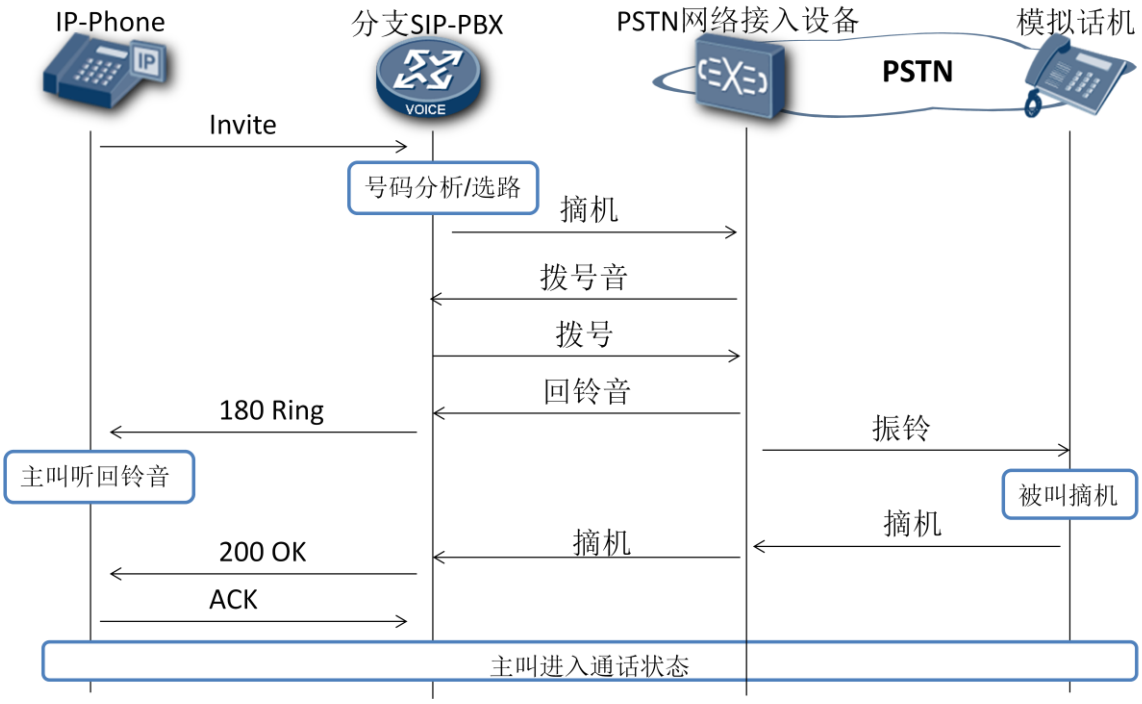
PBX 模式分支拨打总部流程



PBX 模式分支拨打分支流程

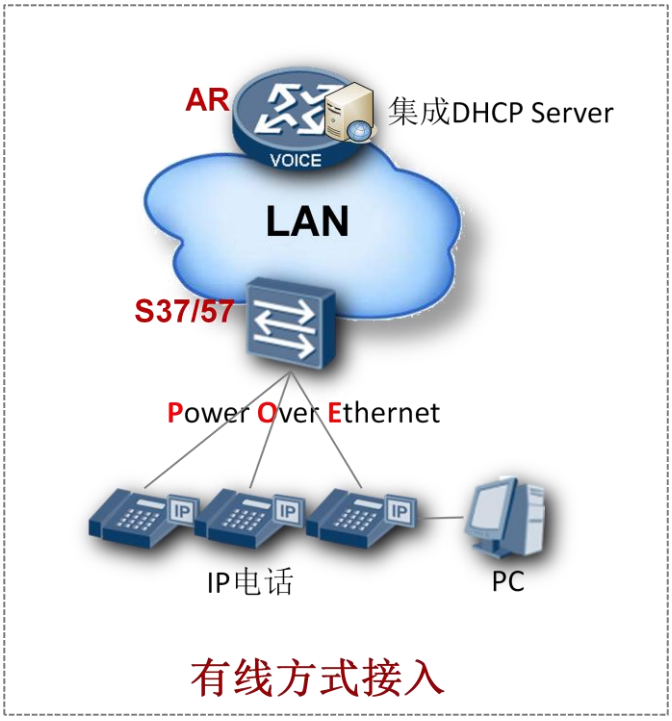


PBX 模式分支拨打 PSTN 外线流程

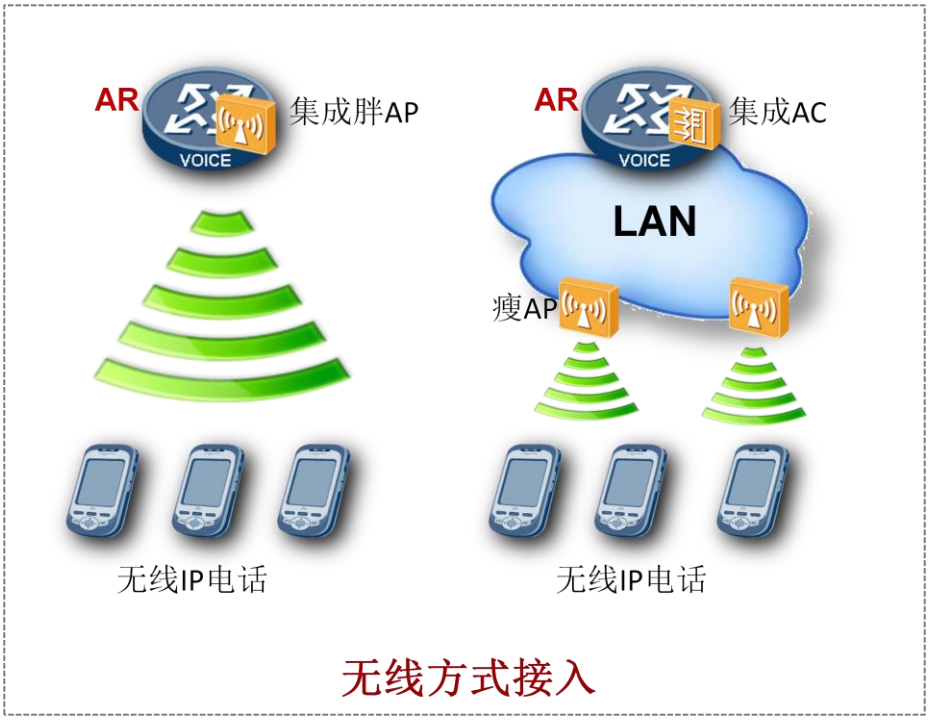


语音终端接入方式

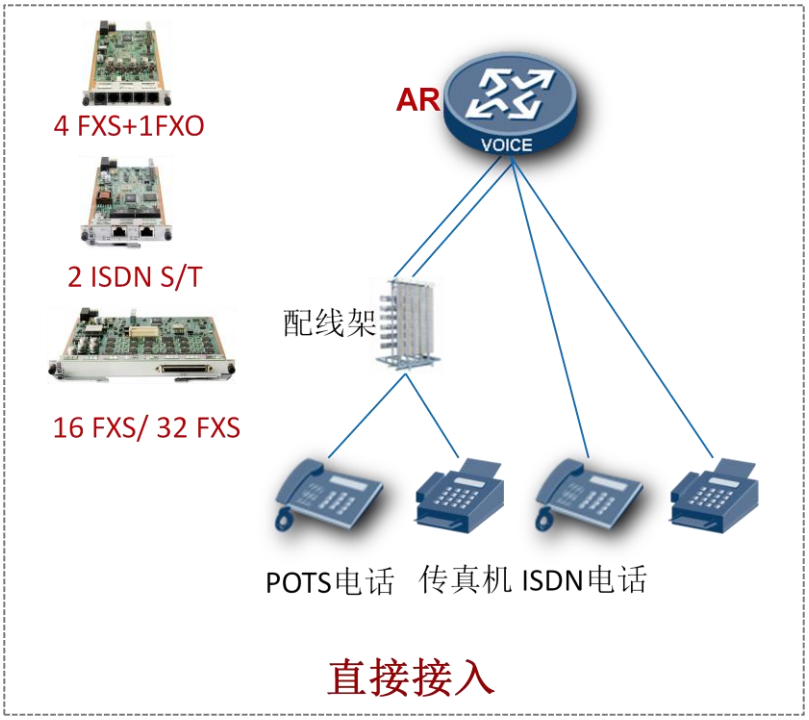
- 有线 IP 电话接入到 S37/S57 交换机上，交换机提供 POE 功能，可对 IP 电话进行供电，简化布线。IP 电话的 IP 地址可以静态配置，也可动态获取，AR 集成 DHCP Server 功能。IP 电话可以提供两个以太网卡，分别接网络设备和 PC，简化布线同时节省布线成本。



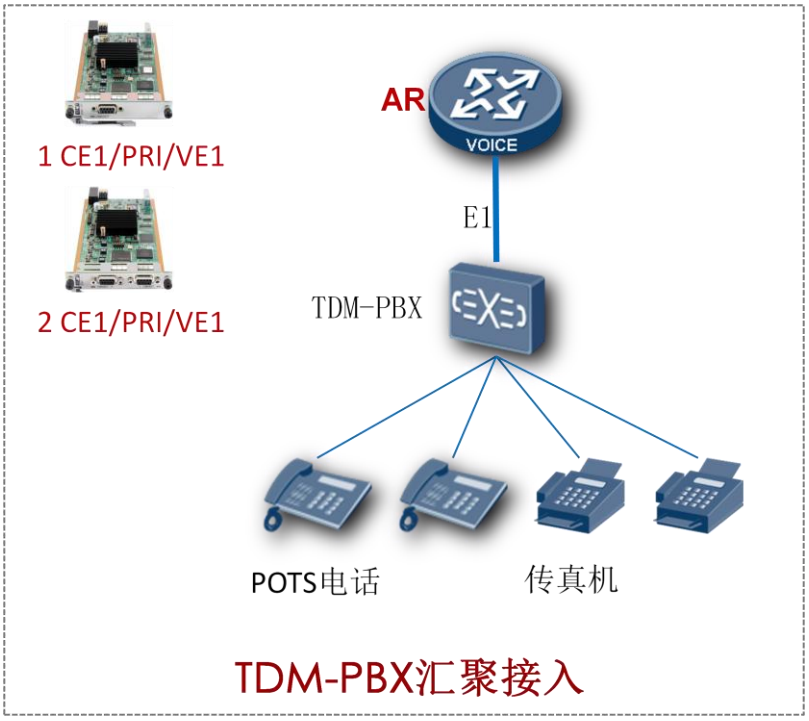
- 微型、小型分支场景下，出口 AR 开启胖 AP 功能，提供无线 IP 电话的 WIFI 接入分支网络。中型、大型分支场景下，通过 AC+瘦 AP 方式扩大 WIFI 覆盖范围。AR 集成 AC 功能，通过 CAPWAP 隧道管理接入 AP。



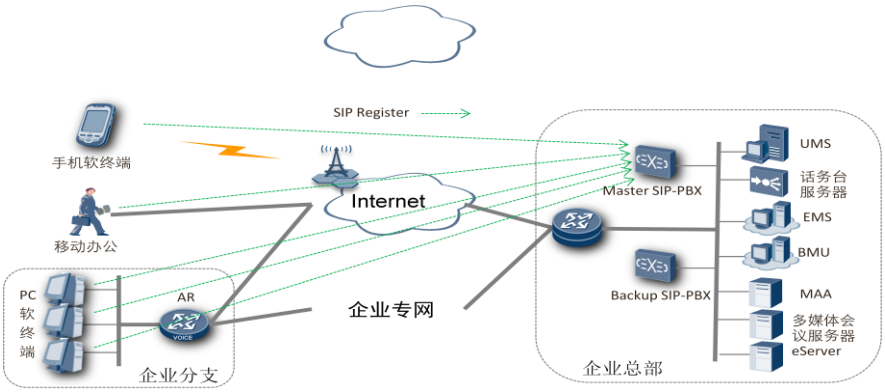
- 模拟话机、传真机通过 FXS、ISDN 直接或通过配线架接入到 AR 设备。AR 设备多种语音板卡，最大可以支持 32 路 FXS 集成在一块板卡上。根据 AR 不同型号产品，可以支持 4~192 个模拟话机直接接入。



- 模拟话机、传真机接入到原先的 TDM-PBX 上，呼叫控制由 TDM-PBX 完成。TDM-PBX 再通过 E1 中继接入到 AR。AR 支持单端口和双端口的 E1 板卡。 E1 的语音功能和数据功能二合一，灵活选择。

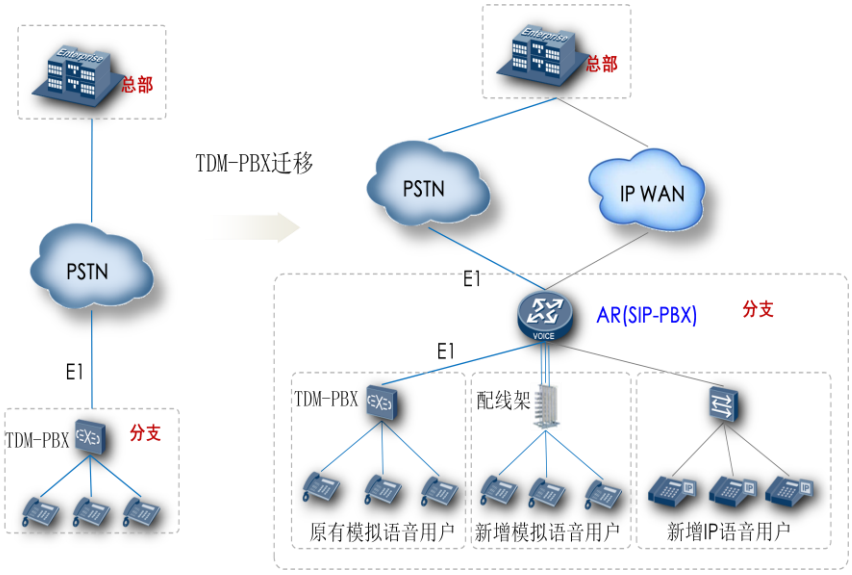


- 企业总部统一部署 SIP 软终端语音通信平台，包括多媒体会议、即时消息、状态呈现、群组消息、企业通讯录、移动接入等功能部件。企业分支的办公 PC、出差员工便携、员工手机终端上可以安装 SIP 终端软件，并且通过有线无线网络注册到总部的 SIP-PBX，客户端软件可以随时随地移动，并且支持 PC 终端和手机终端。企业分支借助总部语音通信平台，企业内部高效沟通，效率提高，降低沟通成本。

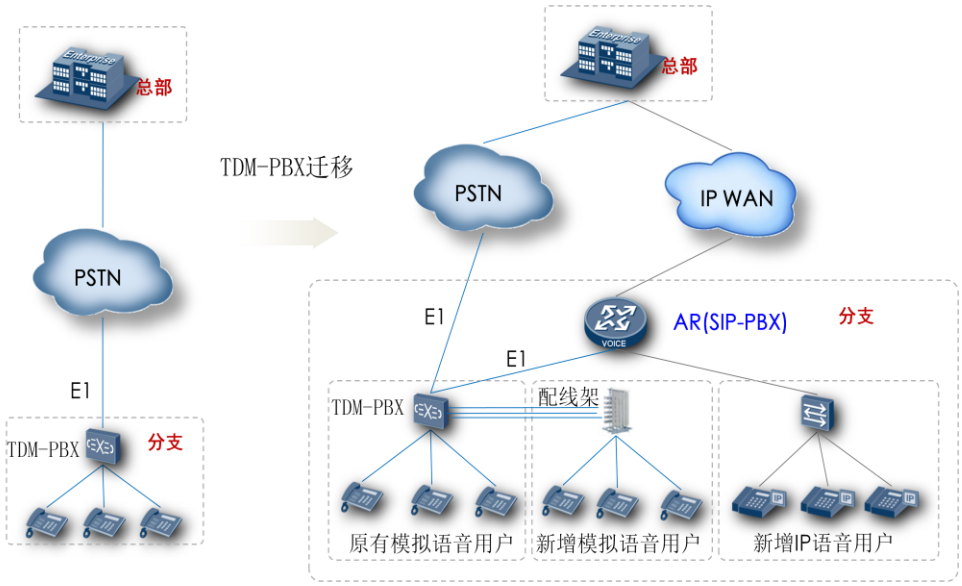


旧通信系统迁移

企业原先通过 TDM PBX 设备接入 PSTN 网络中，现在将语音用户切换到 IP 承载网络上。企业的出口部署多业务路由器，TDM PBX 设备通过 E1 接口连接到 AR 企业多业务路由器设备，使企业的语音用户之间的通信线路走企业的 IP 网络。

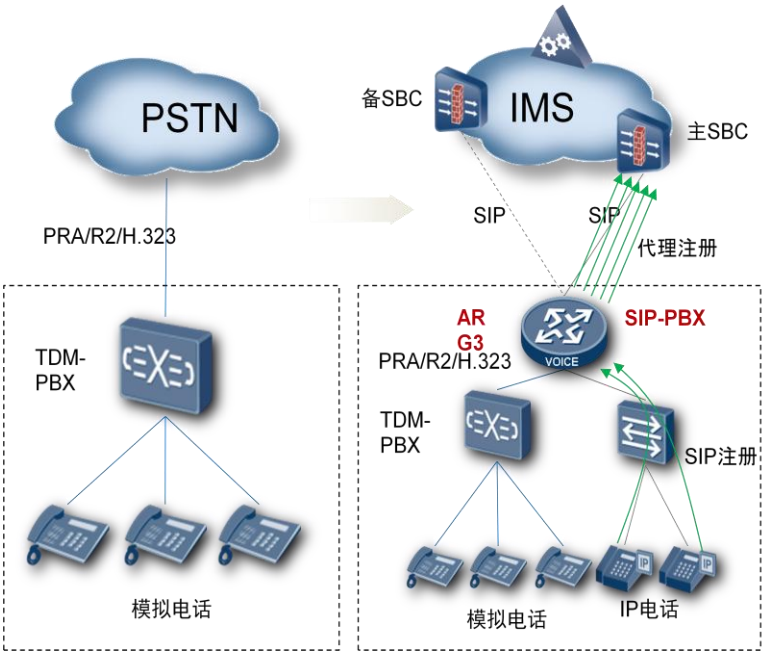


- 分支出口 AR 作为 SIP-PBX，原有连接 PSTN 网络的 TDM-PBX 设备，通过 E1 接口切换接入到 AR 设备上，从而保证原有设备的充分利用。TDM-PBX 性能已经达到上限建议采用此方案，TDM-PBX 只维护原有模拟语音用户，不维护任何新增语音用户。AR 作为 SIP-PBX，所有新增的 POTS 语音和 IP 语音用户均由 AR 进行规划管理。并且统一接入 PSTN 网络和 IP 网络。



- 对于 TDM-PBX 设备下的语音用户比较多，并且 PBX 还有一定扩容能力，建议保留原来的 E1 出局到 PSTN 网络，另外通过 E1 接口中继到 AR 上，实现分支内模拟电话跟 IP 电话互通。AR 路由器作为 SIP-PBX，只管理新增 IP 语音用户。TDM-PBX 和 IP-PBX 分开接入 PSTN 网络和 IP 网络。原有电话系统 TDM-PBX 还具有 30%的扩容能力，建议采用此方案。

分支 IMS 网改



该场景应用于企业分支从 PSTN 网络切换到 IMS 网络，享受 IMS 提供的丰富业务。如何平滑的从 PSTN 网络迁移到 IMS 网络，我们建议采用如下部署：

1、 新增 AR 下挂原先的 PBX 和新增语音用户，上接 IMS SBC。

2、 将传统 TDM PBX 的 PRA/R2 协议转换为 SIP 协议并提供代理注册功能。

3、 分支内部业务由分支 PBX 完成，外呼业务由 IMS 实现。

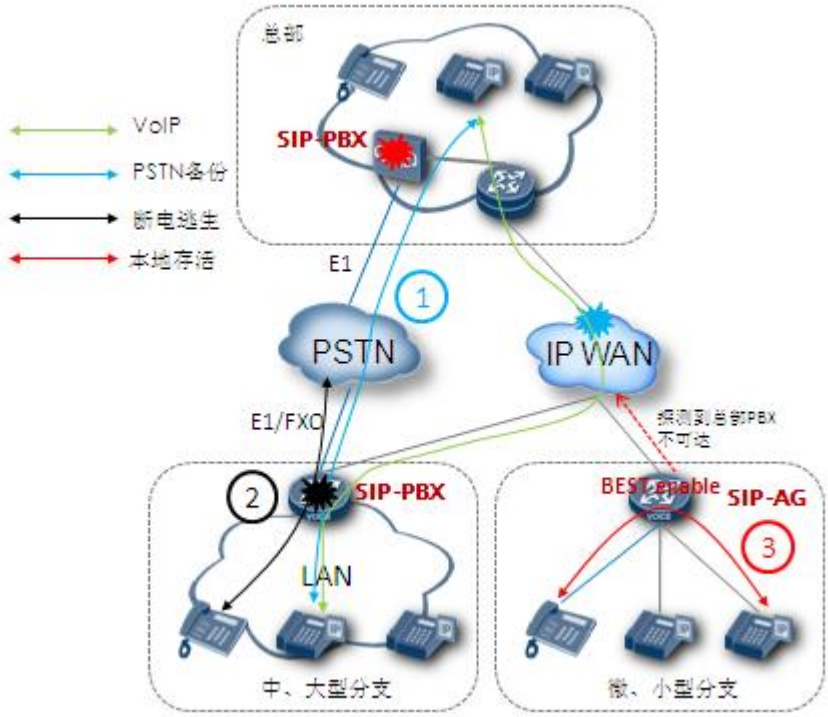
该方案亮点为通过 AR 的代理注册实现有效隔离客户终端。部署主备 SBC 实现异地容灾，实现网络的高可靠性。低成本的 IMS 网改方案，降低企业 IMS 网改成本。

语音 QoS 方案

- IP 话机 QoS：IP 话机支持基于 802.1P 添加语音报文优先级，同时通过 VLAN 区分数据流和语音流，并且支持 Diffserv 流量优先级控制，以保证 IP 话机的信令和数据流可以正常通过企业的 IP 网络。
- 交换机 QoS：交换机入端口配置 Voice VLAN 功能，根据报文源 MAC 自动识别语音流量，添加报文优先级。上行端口根据报文优先级进行 PQ 调度，以保证 IP 话机的心灵和数据流优先通过企业的 IP 网络。
- 路由器 QoS：出口 AR 部署 CBQ 功能，修改语音报文进入 EF 高优先级队列，并配置该队列最小带宽保证，实现当链路拥塞时语音业务能够优先转发并实现最小带宽保证。

语音可靠性方案

传统的语音业务可以通过语音交换机的双上行进行语音业务的保护，当企业从传统语音通信系统切换到 IP 语音通信系统时，语音业务的可靠性保护也需要进行重点考虑，对于 IP 语音通信系统，语音业务的保护需要从语音终端到 IP 承载网络都要进行考虑。



1、 PSTN 长途备份场景：正常情况下，分支跟总部的语音通信为 VoIP。当 IP WAN 网络故障，PSTN 作为备份链路实现跟总部的语音。

2、 断电逃生场景：AR SIP-PBX 模式，断电情况下， 4FXS+1FXO 板卡的 FXO 口转线到相邻 1 路 FXS 口，POTS 话机仍然可以在 AR 断电情况下拔打 PSTN 外线。

3、 BEST 本地存活场景：AR SIP-AG 模式不支持接入 PSTN 网络，当 AG 探测到总部 SIP-PBX 不可达时，启动 BEST 功能，分支内仍然可互相通话。

语音诊断方案

- AR G3 路由器配合 eSight 支持信令跟踪、内外线诊断测试、用户端口主、被动仿真测试等整套诊断测试方案，端到端确定故障范围。
- 操作简便：eSight 诊断维护中心支持面向对象的可视化操作
- 结果准确：端到端的分段测试缩小故障范围，自动给出故障定性结论
- 省时省力：问题解决时间缩短为 0.5 小时，大大节省维护工作量

微软系统集成 AR

微软统一通信利用 OCS 平台将语音、IM、增强状态、音频/视频会议以及电子邮件整合在一起，为用户提供了一种熟悉而全面的通信体验。Microsoft 的统一通信解决方案提供了一种全新的通信方式。

AR 通过 SIP trunking over TLS 和微软 OCS、Exchange 服务相连。为用户提供一个号码能与多个终端进行绑定、语音通话、视频通话、视频会议、状态呈现、统一消息、协同。

UC 基本由 MS OCS 系统提供，AR 功能比较有限，只作为其 PSTN/PLMN 落地网关和向硬话机提供语音服务。通过 fork 呼叫（ OCS 终端和 IP PBX 下接的终端拥有相同同 E.164 号码）允许 OCS 客户端对其下话机进行呼叫控制。

AR 基于 OCS 平台的统一通信方案可以让用户随时随地在有线或无线网络中使用语音、视频、数据等业务，并时时了解自身状态。

OCS 具有人性化的客户体验、清晰的构架以及良好的可扩展性，在业界有较高的认可度。

OCS 系统具有高度的开放性，参照 ECMA CSTA 标准（TR 87、ECMA 269、ECMA 323）来实现。

UC 客户端通过 AR 进行出局呼叫，连接到 PSTN 网络。

华为微软融合 UC 解决方案为用户提供以下功能：

- Dual Forking

  每个用户同时拥有 AR 下的固定电话和 OCS 软终端 MOC（Microsoft Office Communicator），当有电话呼入时，两个终端会同时振铃，用户可选择任意一个进行应答。
- 一个号码能与多个终端进行绑定

  一个号码除了可以绑定固定电话和 MOC 之外，还能绑定手机号码，三个终端可实现同振或顺振，保证呼叫不被错过。
- 语音通话、视频通话和即时消息

  提供便捷、灵活的语音通话、视频通话和即时消息功能，可在当前的交流方式上增加其它的交流方式，如在语音通话的过程中增加视频和即时消息。
- 语音和视频会议

  PSTN 电话、移动电话、AR 下的固定电话和 MOC 能共同参加语音会议；AR 和视频电话可以参加视频会议，提高沟通效率。
- 状态呈现

  通过 MOC 客户端，用户能随时看到好友的状态（包括通话中、空闲、暂时离开、离线等）和位置，方便用户选择最有效的方式与对方通信，提高沟通效率。
- 呼叫控制

  用户可以通过 MOC 对桌面固定电话进行代拨、呼叫前转、呼叫转移、呼叫保持与恢复等操作。
- 协同

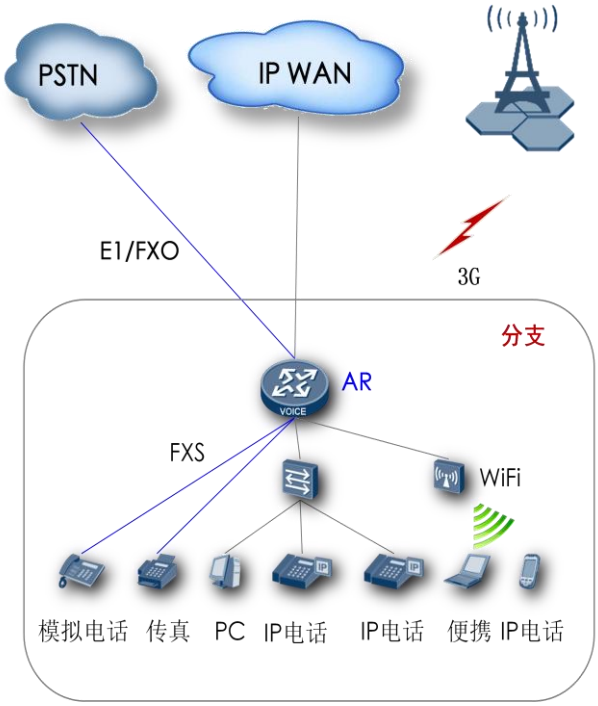
  提供融合了音频、视频的丰富的协同功能，包括应用共享、桌面共享、网页共享、文件共享、会议调查、电子白板、会议录制、会议控制等。
- 可移动性

借助华为微软融合 UC 解决方案，只要能成功连接互联网，用户无论在家里还是在路上，都可以使用 OCS 客户端的即时消息、会议、WEB 协同等功能，非常便捷。

- 统一消息

  当用户有留言，留言可通过 Exchange Server 发送到用户的邮箱，用户可通过 Outlook 客户端或 Outlook Web Access 查看和收听，也可以在普通电话上听取语音留言。

分支 ALL IN ONE



1、 AR 集成 3G，语音、路由功能，实现分支多业务的统一接入，降低企业维护工作量，节省企业投资成本。

2、 AR 工作在 SIP-PBX 模式，连接模拟话机和 IP 话机，实现分支语音业务。

3、 便携、无线 IP 电话通过 WIFI 接入网络，并且安装 SIP 客户端软件，实现移动语音。

语音基本和补充业务

业务类别	业务子类	业务描述
基本业务	-	• 基本通话 • 传真业务 • 号码变换 • 智能路由 • CDR 功能

业务类别	业务子类	业务描述
补充业务	主叫识别	• 主叫号码显示 • 主叫号码显示限制
	呼叫保持	• 双通话业务 • 呼叫等待 • 呼叫转移 • 三方通话 • 呼叫前转
	呼叫控制	• 选择呼叫拒绝 • 选择呼叫接受 • 匿名呼叫拒绝 • 免打扰 • 呼叫拦截
	群组业务	• 同振 • 顺振 • 同组代答 • 指定代答 • 一机多号 • IVR 排队
	个性业务	• 短号呼叫 • 区别振铃 • 缩位拨号 • 闹钟提醒 • 查号业务

语音一号通业务

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，被叫用户的座机号，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。一号通业务的优点：

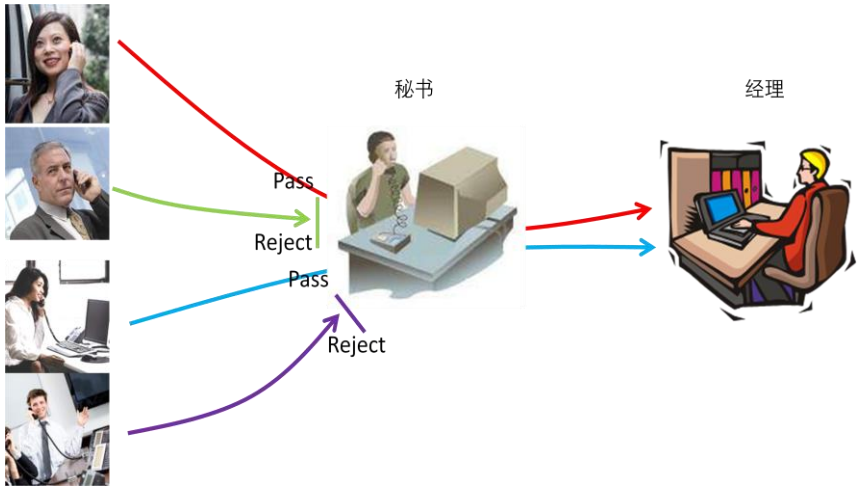
1、 一个号码：无需再记多个号码，提高沟通效率。

2、 一次搞定：只要一次拨号就能够找到对方

3、 方便接听：可以用固定电话、手机、PC 接听。

秘书业务

秘书业务允许用户指定另一部电话（即秘书）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。用户通过秘书业务，可以让秘书接听并过滤来话，避免不必要的打扰。



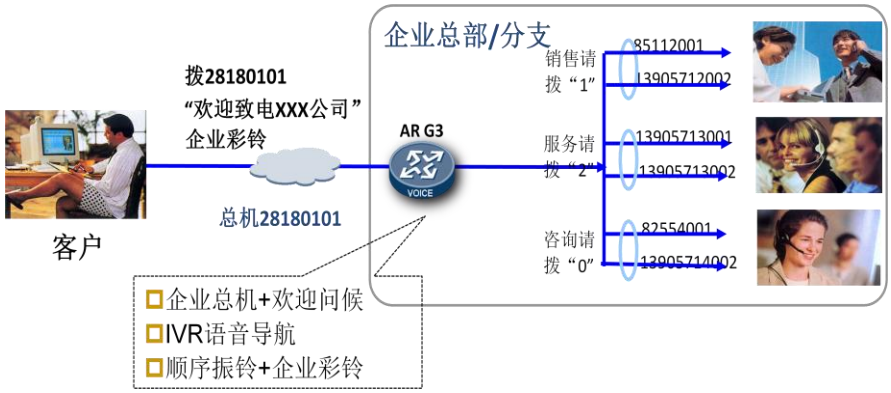
IVR 语音导航

IVR 导航业务是在自动话务员业务的基础上，提供 IVR 提示音的菜单定制和提示音定制功能，灵活的满足企业定制化的需求，提升了用户体验。IVR 语音导航给客户带来如下价值：

1、 联系方便，客户只需记住一个号码。。

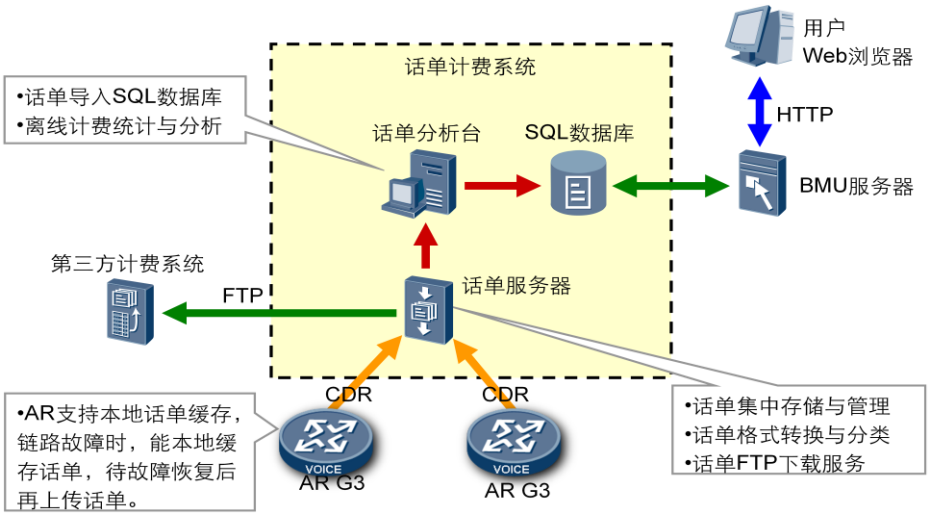
2、 提升形象，企业对外公布总机号码。

3、 巩固客户，员工流动业务不受影响。



话单（CDR）和计费

CDR(Call Detail Record：计费数据记录)业务指通过系统可以实时记录并输出用户的呼叫详细记录，可以通过第三方工具分析 CDR 记录数据，使用户能够及时获知用户呼叫过程中的费用。



3.3 Wlan

3.3.1 技术背景

WLAN（Wireless Local Area Network）是指利用高频射频信号（例如 2.4GHz 或 5GHz）作为传输信道的无线局域网。

802.11 是 IEEE 在 1997 年为 WLAN 定义的一个无线网络通信的工业标准。此后这一标准又不断得到补充和完善，形成 802.11 的标准系列。例如比较重要的 802.11、802.11a、802.11b、802.11e、802.11g、802.11i、802.11n 等。其中基于 802.11b 标准的有时也被称为 Wi-Fi 标准。而 802.11n 标准兼容 802.11a/b/g，带宽优势明显，已经成为当前的主流技术。而随着 802.11ac 技术的出现，必将引领无线业务进入千兆时代，为用户带来千兆级别的接入速度。

802.11 标准简介

标准名称	发布时间	工作频率	理论速率	实际速率	备注
802.11b	1999	2.4GHz	11Mbps	6Mbps	早期标准
802.11a	1999	5.0GHz	54Mbps	22Mbps	应用很少
802.11g	2003	2.4GHz	54Mbps	22Mbps	早期标准
802.11n	2009	2.4/5.0GHz	150Mbps	75Mbps	结合MIMO技术，理论速率600Mbps
802.11ac	2012	5.0GHz	1Gbps	400～500Mbps	802.11n 下一代标准
802.11ad	发展中	60GHz	7Gbps	发展中	面向家庭高清娱乐设备

企业无线分支网络的发展及设计需求

随着技术的发展和大量移动终端的出现，企业分支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。

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、计费的需求。

3.3.2 WLAN 基本概念

WLAN 网络在部署过程中，根据不同的需求有多种实现形式，根据网络架构分为：

- 自治式架构（即 FAT AP 或胖 AP）

- 集中式架构（即 FIT AP 或瘦 AP）

自治式架构和集中式架构两种网络结构比较如 0 所示。

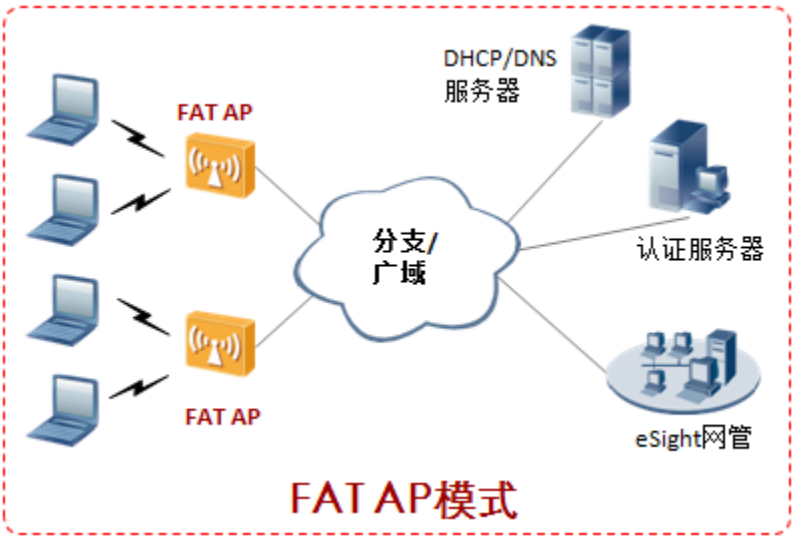
自治式架构和集中式架构比较表

项目	自治式架构	集中式架构
适用场景	微型企业、个人	新生方式，增强管理
安全性	传统加密、认证方式，普通安全性	基于用户位置的安全策略，高安全性
网络管理	每 AP 需要单独下发配置文件	AC 上统一配置，AP 本身零配置，维护简单
用户管理	类似有线，根据 AP 接入的有线端口区分权限	虚拟专用组方式，根据用户名区分权限，使用灵活
WLAN 组网规模	L2 漫游，适合小规模组网	L2、L3 漫游，拓扑无关性，适合大规模组网
增值业务能力	实现简单数据接入	可扩展丰富业务

自治式架构

该架构下 AP 实现所有无线接入功能，不需要 AC 设备形态，如下图所示。

WLAN 自治式架构图



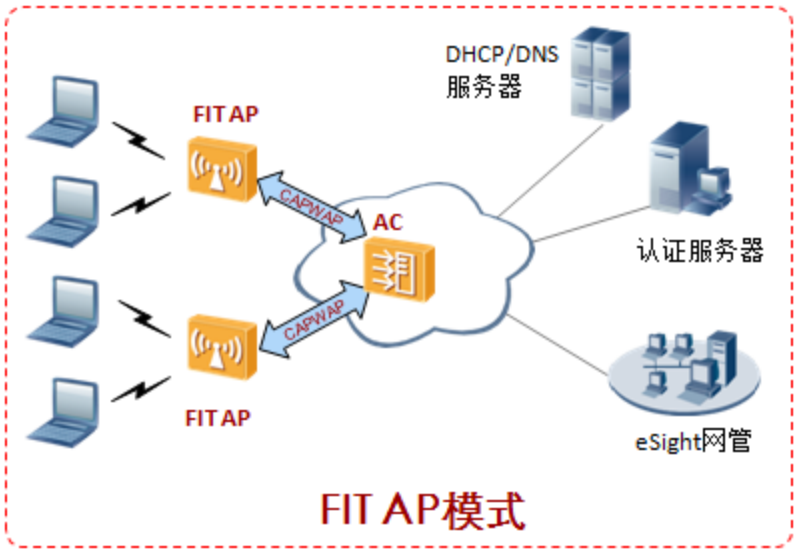
WLAN 早期广泛采用自治式架构，随着企业大量部署 AP 后，对这些 AP 进行配置、升级软件等管理工作将给用户带来很高的操作成本，管理成本提高，自治式架构应用逐步减少。

集中式架构

该架构通过无线控制器（AC）集中管理、控制多个 AP，如 0 所示。所有无线接入功能由 AP 和 AC 共同完成：

- 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（Intrusion Detection Systems）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等。

WLAN 集中式架构图



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。

所有无线接入功能由 AP 和 AC 间共同完成。集中式架构是企业网、运营商等 WLAN 方案的主要架构，便于集中管理、集中认证和实施安全策略。此种方案为目前企业网通用方案。

在 FIT AP 网络架构下，又有如下划分：

- 根据 AC 部署方式，分为集中式和分布式
- 根据 AC 部署位置，分为旁挂和直路

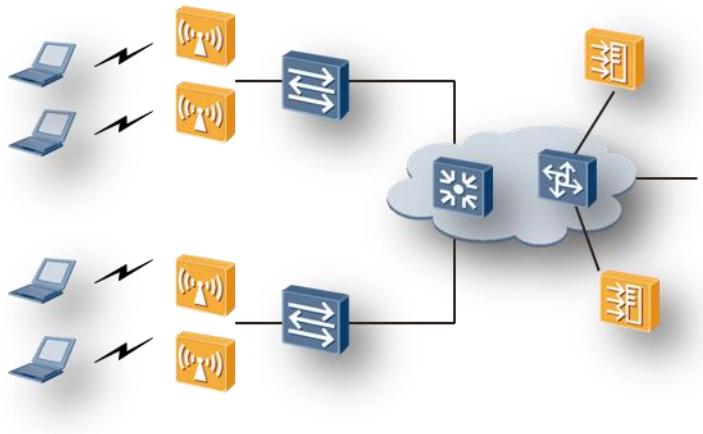
- 根据 AC 硬件体现形式，分为集成 AC 和独立 AC
- 根据业务转发形式，分为本地转发和集中转发

根据 AC 的部署方式，网络可分为集中式 AC 部署和分布式 AC 部署。

集中式 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）。

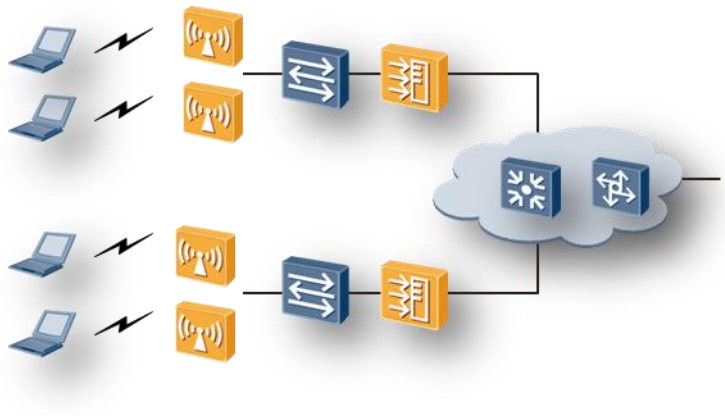
集中式 AC 部署示意图



分布式 AC 部署

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。

分布式 AC 部署示意图



AC 的两种部署方式的优劣势对比如下图所示。

集中式 AC 与分布式 AC 优缺点对比表

AC 部署方式	优点	缺点
集中式	• 节省投资 • 容量管理更简单有效，成本效益高 • 无线业务终结点少，便于管理 • 漫游部署简单、高效 • 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	• 投资成本高 • 需要部署 AC 间漫游（除非各 AC 所在的区域间不考虑漫游） • 运维成本高

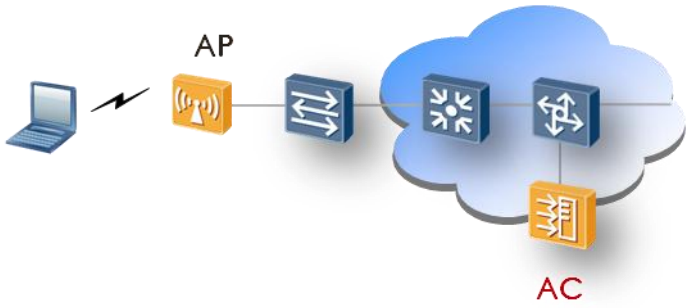
根据 AC 在网络上所处位置，可分为 AC 旁挂和 AC 直路。

旁挂

旁挂方式是指将 AC 部署在用户网关设备（汇聚或核心交换机）一侧，实现对用户网关设备下所有 AP 的管理。

旁挂方式主要用于原有网络汇聚/核心设备非华为设备的场景，目前主要用于网络改造、或者新建大、中型园区网络场景。

AC 旁挂示意图

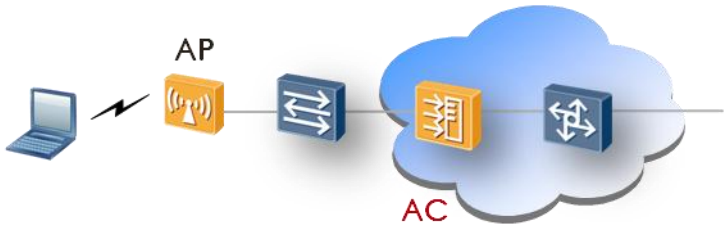


直路

直路方式是指将 AC 部署在 AP 与用户网关设备（汇聚或核心交换机）之间，实现对下辖所有 AP 的管理。

直路方式主要用于新建中、小型园区网络或原有网络汇聚/核心设备为华为设备的场景。

AC 直路示意图



根据 AC 硬件体现形式，可分为集成 AC 与独立 AC

集成 AC

集成 AC 方案指不采用单独的 AC 硬件设备，而是采用在交换机中集成的 AC 硬件插卡，来实现对交换机下所有 AP 的管理。

在集成 AC 方案中，采用集中式架构（FIT AP 架构），使用 FIT AP 来负责无线终端的接入。使用集成的 SPU 板卡作为 AC，负责完成对 AP 设备的管理。

独立 AC

独立 AC 方案是指采用单独的 AC 硬件设备，通过直路或者旁挂方式实现对于所有 AP 的管理。

在独立 AC 方案中，采用集中式架构（FIT AP 架构），使用 FIT AP 来负责无线终端的接入。使用独立的 AC 设备完成对 AP 设备的管理。

集成 AC 和独立 AC 优缺点比较如下图所示。

集成 AC 和独立 AC 优缺点比较表

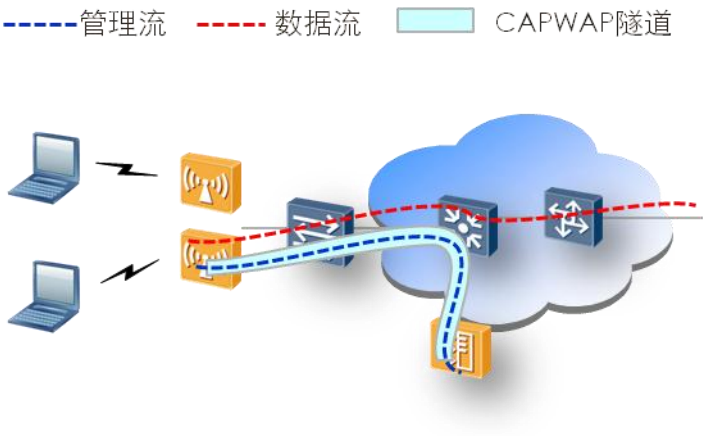
AC 硬件形式	优点	缺点
集成 AC	部署简便；价格较低。	在接入用户数方面略差
独立 AC	可以实现大容量、高性能的 WLAN 网络部署。	价格较高，成本高。

根据转发模式不同，可分为本地转发与集中转发。

本地转发

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。

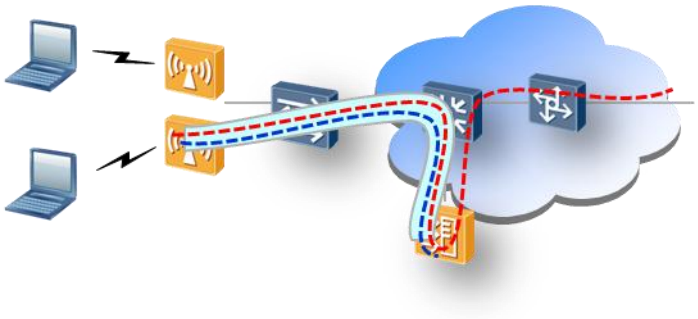
本地转发示意图



集中转发

也称作隧道转发。业务数据报文由 AP 统一封装后到达 AC 实现转发，AC 不但进行对 AP 管理，还作为 AP 流量的转发中枢。即 AP 管理流与数据流都封装在 CAPWAP 隧道中到达 AC。

隧道转发示意图



本地转发与集中转发优缺点对比如 0 所示。

本地转发与集中转发优缺点对比表

转发方式	优点	缺点
本地转发	设备署简单，数据流量不经过 AC，AC 负担小。	-
集中转发	数据流量和管理流量全部经过 AC，可以按用户需求规划安全监管策略。	AC 设备数据压力较大，对 AC 设备本身处理能力要求较高。

3.3.3 WLAN 网络规划

IP 地址规划

也称作隧道转发。业务数据报文由 AP 统一封装后到达 AC 实现转发，AC 不但进行对 AP 管理，还作为 AP 流量的转发中枢。即 AP 管理流与数据流都封装在 CAPWAP 隧道中到达 AC。

AC 的 IP 地址

AC 用于管理 AP，IP 地址一般通过静态手工配置。

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下图所示。

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

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。

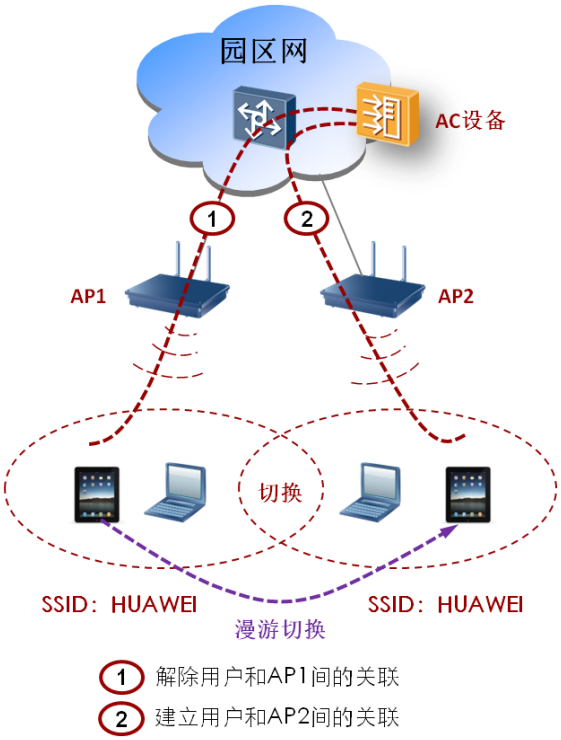
VAP 构建

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。

用户漫游切换示意图



如上图所示，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。

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。

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。

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。

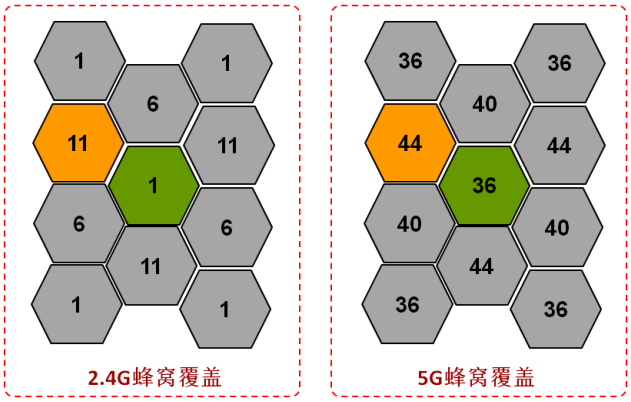
AP 支持手动和自动两种方式设置工作信道。设置为自动方式后，一旦检测到信道冲突 AP 具有信道自动调整功能，建议 AP 采用自动设置工作信道方式，避免手动设置后一旦信道冲突将导致无法切换信道的问题。

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。

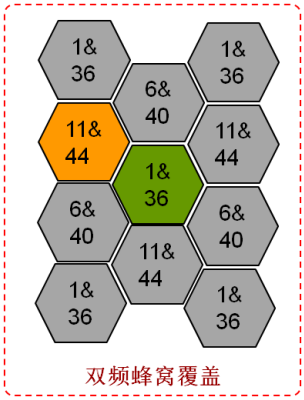
射频信道覆盖

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 5.8G 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。

单频信道规划示意图



双频信道规划示意图



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。常采用无线空口做 WMM 调度，有线侧进行优先级映射，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。

- 流分类

  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。

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

- 准入控制 CAC

  CAC 的基本原理是客户端只有获得 AP 的批准，才能以高优先级的 AC 发送数据，否则只能使用低优先级的 AC，保证了已经获得批准的客户端能够获得需要的带宽。

  准入控制 CAC 部署建议：对 AC-VO（语音流）、AC-VI（视频流）进行准入控制，AC-BE（尽力而为流）、AC-BK（背景流）无需准入。

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，再实现到隧道优先级 Tunnel-802.1P、Tunnle-TOS 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。

3.3.4 WLAN 在分支网络中的应用

微型分支无线接入

微型分支无线接入特点：

- 无线接入

  微型分支规模在十人以下，建议采用 AR151W/1220W 胖 AP 接入。

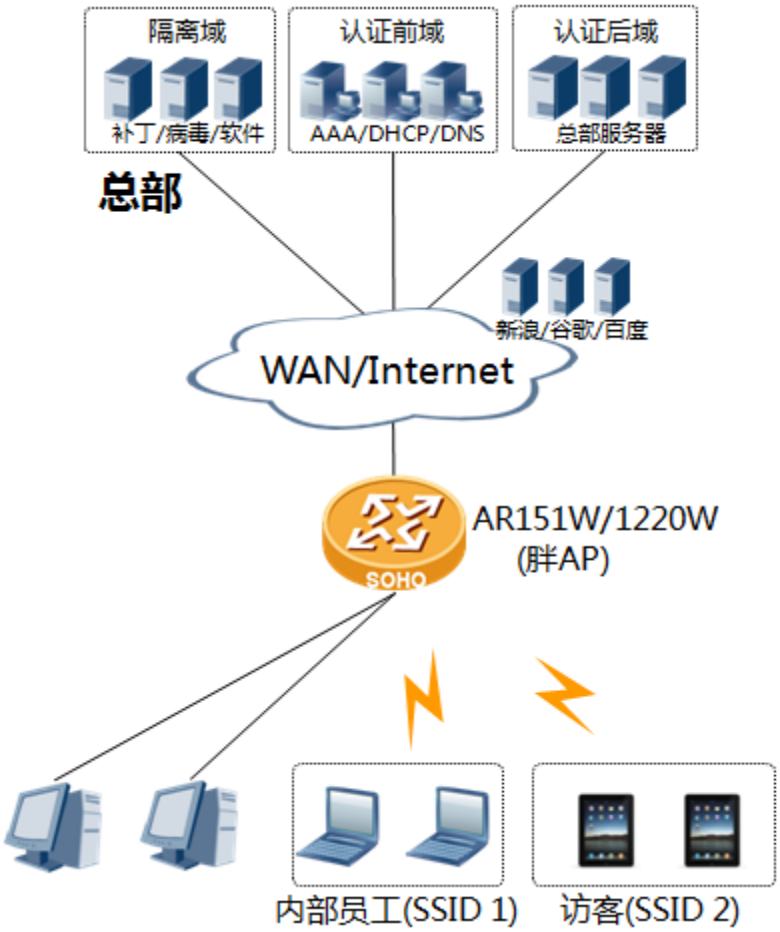
- 内外用户隔离

  内部员工与访客分别接入到不同 SSID，二层 VLAN 隔离；若有需要，可通过 AR 路由器的安全域特性实现三层隔离。

- 安全认证

  对于企业分支用户采用 802.1x 认证，访客需先申请账号/密码，然后 Portal 认证，认证后，只开放因特网/总部 DMZ 服务器权限。

对于独立小企业，由于无远程认证服务器，内外部用户均采用 WPA2 认证。



小型分支无线接入

小型分支无线接入特点：

- 无线接入

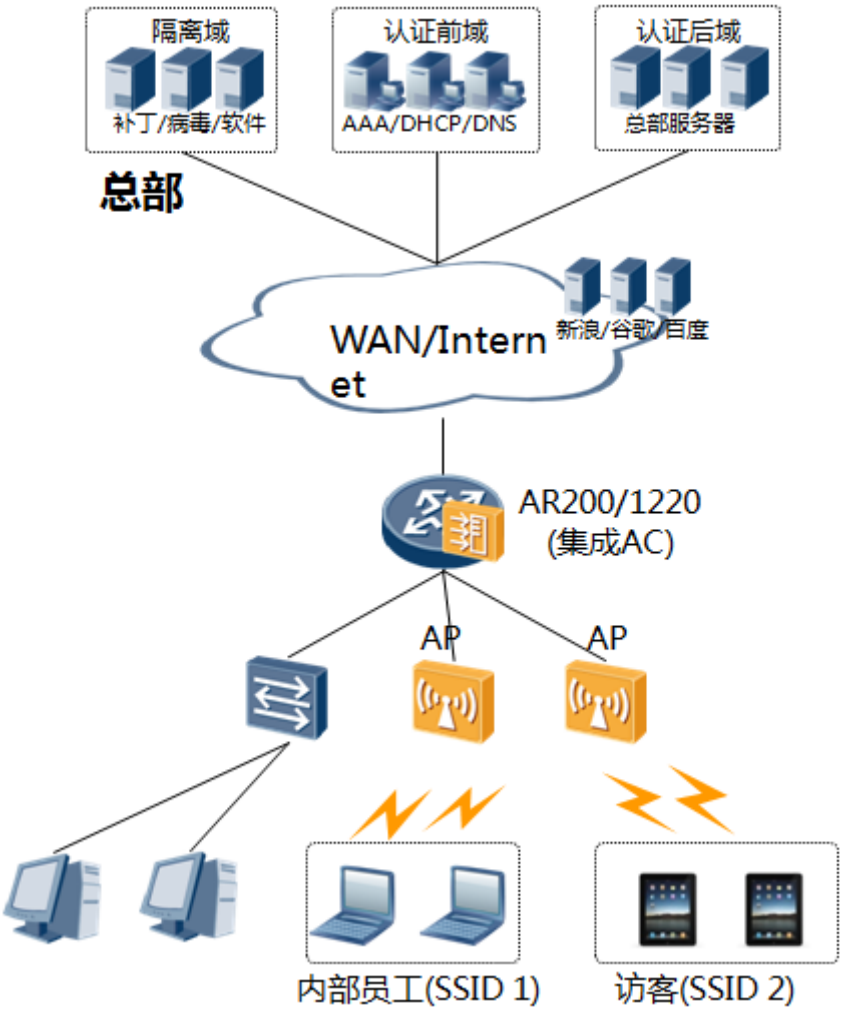
  小型分支规模在 10~50 人，小型分支地域跨度较大，单个胖 AP 无法提供接入需求，建议采用 AR200/1220 搭配 AP 接入。

- 内外用户隔离

  内部员工与访客分别接入到不同 SSID，二层 VLAN 隔离；若有需要，可通过 AR 路由器的安全域特性实现三层隔离。

- 安全认证

  内部用户 802.1x 认证。访客需先申请，再 Portal 认证，只开放因特网/总部 DMZ 服务器权限。



中型分支无线接入

中型分支无线接入特点：

- 无线接入

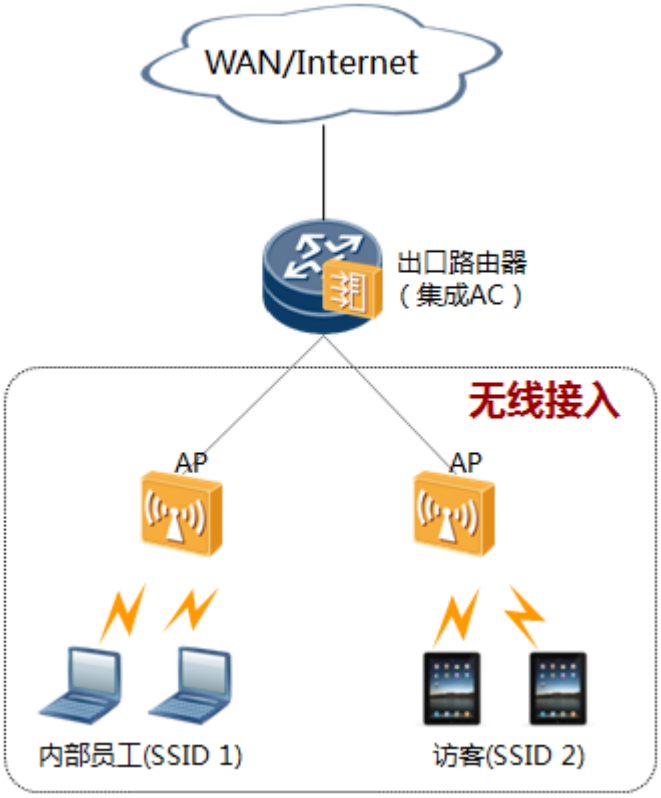
  中型分支规模在 50~250 接入点，AR(集成 AC)可以管理 64AP+512 无线用户，故采用 AR2200 搭配 AP 方案。

- 内外用户隔离

  内部员工与访客分别接入到不同 SSID，二层 VLAN 隔离；若有需要，可通过 AR 路由器的安全域特性实现三层隔离。

- 安全认证

  内部用户 802.1x 认证。访客需先申请，再 Portal 认证，只开放因特网/总部 DMZ 服务器权限。



WLAN 接入认证

WLAN 接入认证特点：

- 认证方式

  内部员工采用 802.1x 认证，更安全。

  外部访客采用 Portal 认证，免装客户端。

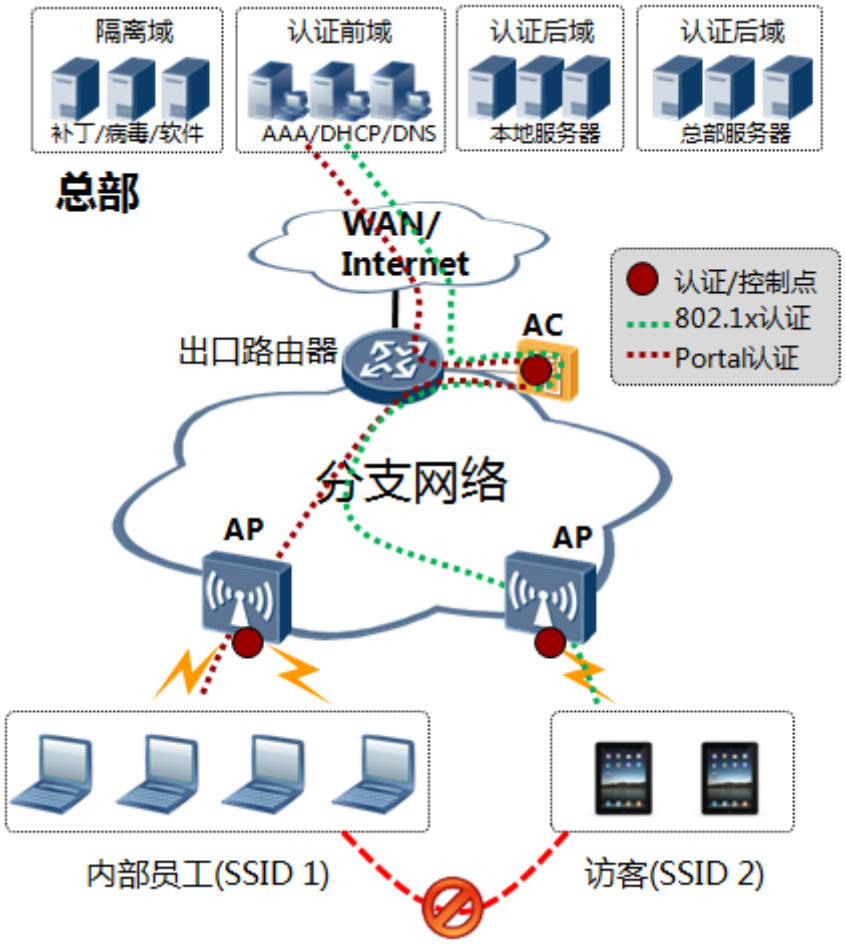
- 资源授权

  对内部员工根据需要办公开放资源。

  对访客只开放 Internet 和 DMZ 资源，禁止访问认证后域的企业内部资源

- 内外隔离

  内部员工与访客分别接入不同 SSID，二层 VLAN 隔离，三层归属不同安全域隔离



3.4 运维

3.4.1 分支运维发展面临的挑战

企业分支运维发展所面临的挑战：

- 分支设备类型众多，包括路由器、接入交换机、语音设备、无线设备，且设备隶属多厂商，很难进行统一管理。
- 总部与各个分支存在不同的管理人员，管理不同地域的设备，且要求有不同的管理权限，如何实施职、权、责精细化管理也是个难题。
- 分支与总部间接入方式众多，如各种 VPN 方式、专线、WLAN、3G 等，安全性要求高，如何对各种接入设备进行统一的、安全的管理是个难题。
- 对整个网络拓扑、网络设备缺乏一体化的、可视化的管理。
- 不能及时发现网络故障，出现故障时定位困难，不能及时解决，网络运营成本高
- 不能快速发放、开展新业务，不能快速提供新的 IT 服务。

3.4.2 分支网络管理的融智方案

华为公司提出融智 eSight 解决方案，是基于标准化、协同、智能联动的分支网络解决方案，具备如下基本特点：

- IT + IP 设备统一管理。提供多厂商设备统一管理。
- 支持分级管理。分域管理。分权管理。
- 在基础管理管理上，提供一体化的增值业务管理：MPLS VPN 管理、IPSec VPN 管理、WLAN 管理。
- 全网设备的自动发现、IP 拓扑与二层拓扑、机房机架拓扑统一展示。
- 基于模板的、可定制的性能数据采集，阈值越限时发送告警。在网络健康趋势恶化之前，主动采取措施。内置语音故障诊断。
- 智能配置工具，端到端的批量配置部署。U 盘开局、Zero-Touch 自动配置。

华为公司提出融智 eSight 解决方案的网络全景图如下：

- 设备可视

  可视化管理分支交换机、路由器、打印机等设备，网络问题实时呈现。

- 流量可视

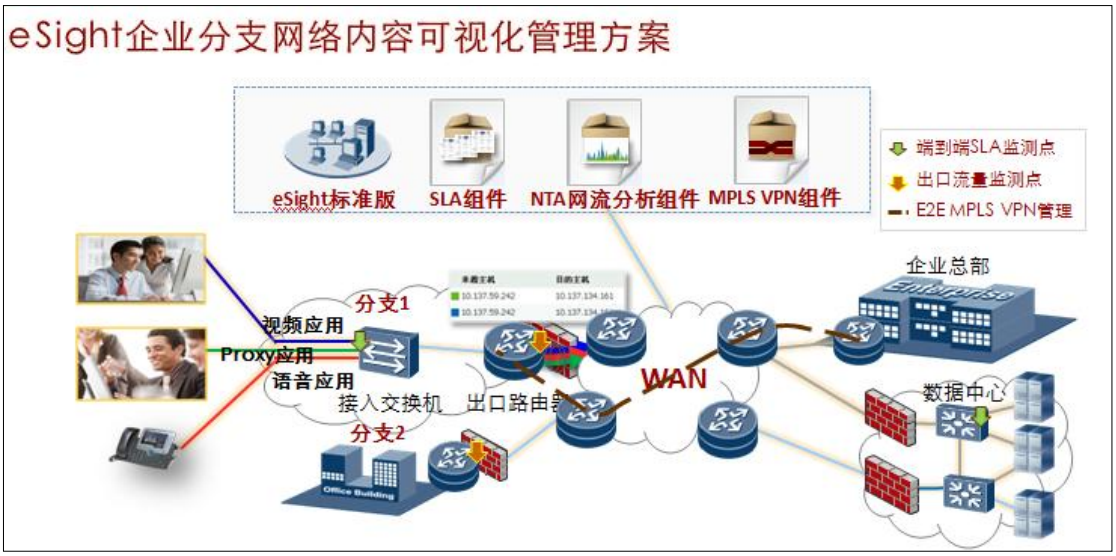
  分支流量精细化管理，TopN 应用流量，TopN 主机信息一目了然，让网络流量变立体，帮助企业分支流量可视、异常可查、规划可依

- 质量可视

  端到端可视化 SLA 评估，与设备 NQA 完美配合，对网络数据报文的时延、丢包、抖动等进行评估，及时发现网络问题，保障分支办公体验。

- 业务可视

端到端 MPLS VPN 可视化管理，业务视图，MPLS 业务 SLA 可视，业务->设备->端口一站式故障诊断，降低企业运维要求



eSight 对于企业分支网的运维，在设备管理上能支持网络设备、服务器、IT 应用的管理，支持对多厂商设备管理，实现单一网管能够运维多厂商设备。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，可以轻松实现分支网络日常维护。融智 eSight 具有如下的技术亮点：

- 轻量级、组件化架构

  基于 B/S 和 SOA 架构，瘦客户端，功能模块组件化解耦，便于在企业网不同场景下面灵活组合；并且网络规模伸缩性强，定位可高可低。

- 设备适配技术

  基于一个稳定的版本加载不同的适配包实现多种设备的管理能力，使得在确保核心功能的稳定性同时达到快速适配新的设备类型及版本的目的。

- 多版本形式

  面对不同的分支网络规模、不同的企业客户，需要有不同的产品形式满足，既要能满足中小企业的中低端网管需求，又要能满足大网络规模的企业网管需求，需要有多种版本形式满足不同客户的需求。

- 易于二次开发

  eSight 能够提供二次开发能力，使代理商或者合作方能够基于该平台进行二次开发和定制，满足不同客户不同场景的要求，并提供系统接口与第三方系统集成。

- 多业务管理

  eSight 不仅在网络资源管理的基础上实现了拓扑、故障、性能、配置、安全等管理功能，而且还可以作为其他业务管理组件的承载平台，共同实现管理的深入融合联动。软件通过流程向导的方式告诉用户如何使用功能，为用户提供了精细化的管理。

通过 WLAN 业务管理主机能帮助用户快速完成无线网络部署，提供网络设备、WLAN 无线设备实现有线、无线一体化管理。为用户日常运维及网络调整提供了依据，极大提升网络管理效率。BGP/MPLS VPN 业务管理，实现对 VPN 业务的监控和部署管理。

3.4.3 融智 eSight 在分支网络中的应用

1、 安全管理

安全管理实现对网管系统本身的安全控制，通过对用户、角色、权限和操作集等管理，保证网管系统的安全。安全管理基于角色模型，从管理设备范围、操作范围两个方面对用户权限进行控制。

2、 日志管理

日志信息记录了用户进行的一些重要操作，用户可以查看、过滤日志列表，还可以详细查看某条系统日志的内容。支持管理操作日志、安全日志和系统日志，提供提示、一般和危险三种级别的信息。

3、 网元管理

网管对设备的管理，包括设备添加、删除。提供子网的管理方式，用户可以根据实际设备的物理位置，划分不同的子网对设备进行区域管理。

添加设备作为网管管理的基础，用户可通过多种方式完成网管添加设备的过程。支持三种方式的网元添加方式：手动添加设备、网段自动发现设备、文件批量导入设备。

- 网元监控

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

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，如下表所示。

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。
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。
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。

设备类型	支持的功能
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。

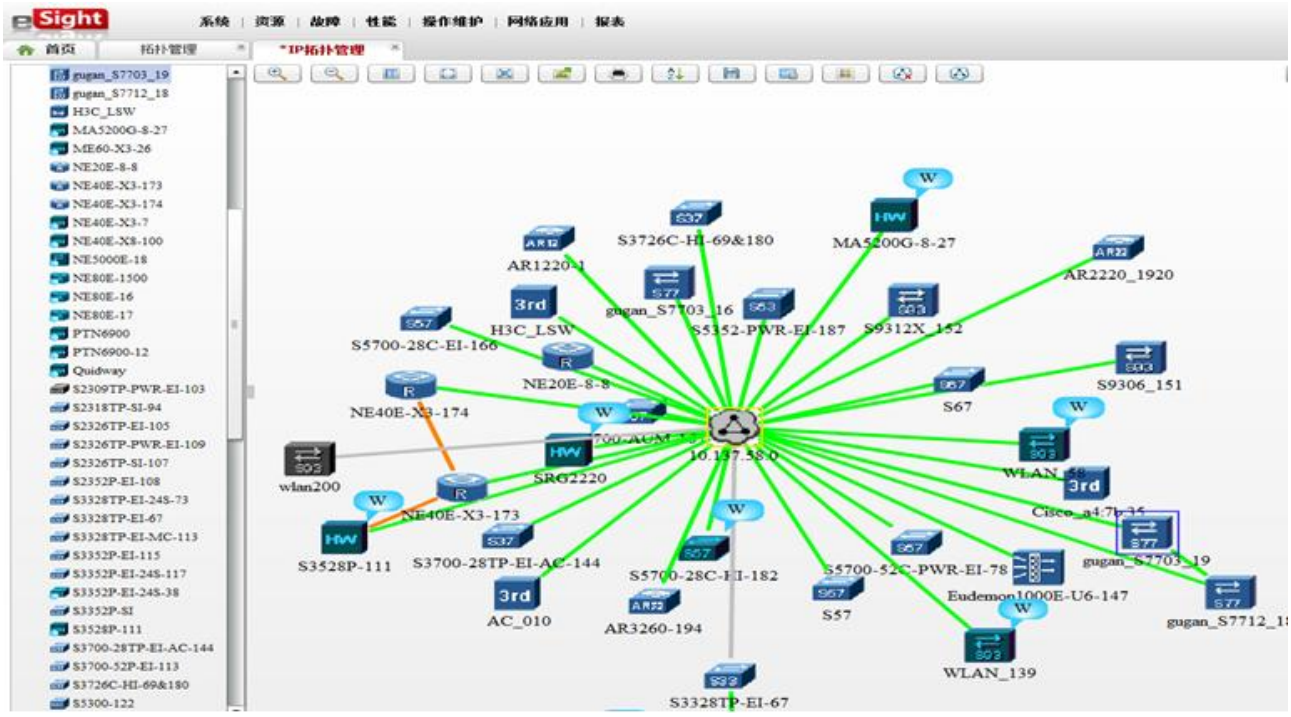
1）使用简单配置框架实现接口、路由等配置。

2）使用智能配置工具进行设备单点配置。

3）交换机、AR 和安全设备通过 Web 网管进行单点配置。

4、 拓扑管理

eSight 以左树右图的方式组织整个视图，其中左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。如下图所示。



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能力。

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功能。

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。

5、 告警管理

告警管理是对网络中的异常运行情况进行实时监视，通过告警实时浏览、告警操作、告警规则设定（屏蔽规则、声音设定）、告警远程通知等手段，便于网络管理员及时采取措施，恢复网络正常运行。

告警管理是对网络中的异常运行情况进行实时监视，通过告警监控板、实时告警浏览、历史告警浏览、事件列表查看等功能对网络故障进行监控。

用户可以根据需要设定告警的远程通知规则、告警屏蔽规则和告警的声音。丰富网络管理员优化网络管理方法。

包括：告警浏览提供多个界面对不同的告警数据进行浏览；告警确认与清除；告警远程通知等功能。

6、 性能管理

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

1）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。

2）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。

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。

7、 资源查看、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。

8、 配置文件管理

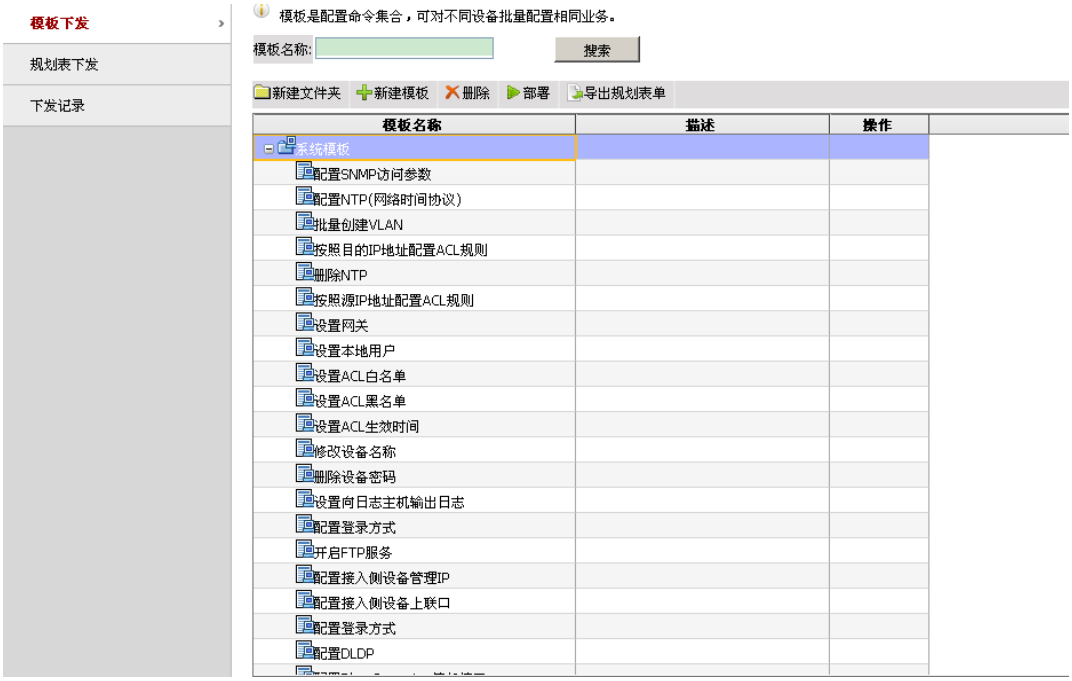
eSight 提供配置文件管理和备份功能，可以快速的进行文件备份和设备登陆管理。同时还提供系统巡检工具，能够定时的对设备进行自检，减轻网络维护人员的工作量。

9、 智能配置

智能配置工具用于对华为设备进行业务配置，支持配置模板和规划表对设备批量下发业务配置。模板主要用于对多个网元进行相同业务配置的批量下发；规划表主要用于对多个网元进行相似业务配置的批量下发。

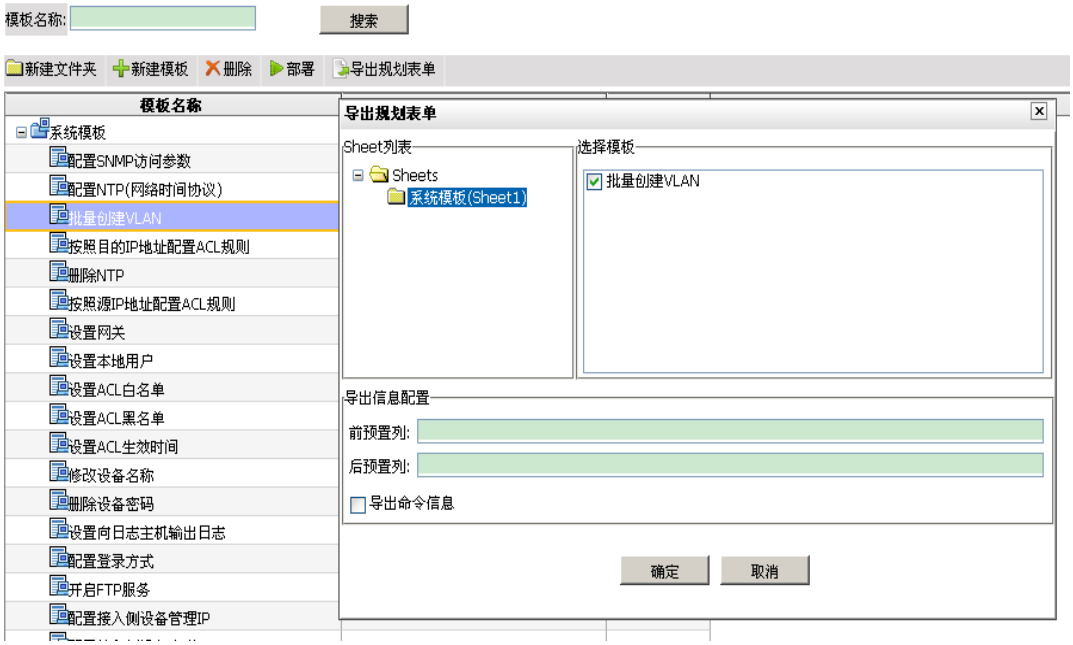
- 模板下发

通过配置模板方式对华为设备实现批量配置下发，用户也可以自定义配置模板，以向导方式下发设备，并且可进行命令验。如下图所示：



- 规划表下发

通过规划表方式对华为设备实现批量配置下发，用户在导出的规划表中填写业务配置参数，导入智能配置工具后以向导方式下发设备。如下图所示：



10、 第三方设备定制

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。

- 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。

- 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，并在在告警管理界面上进行显示。

- 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。

- 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。

- 设备配置文件定制

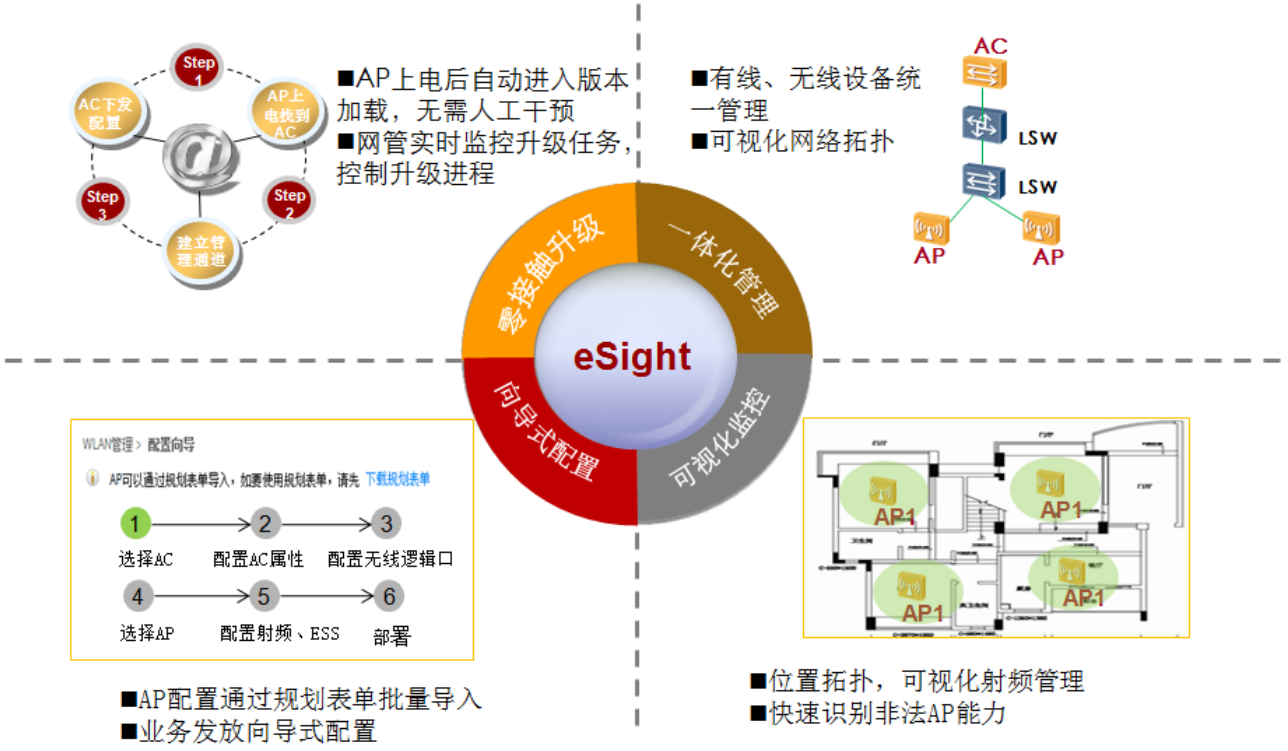
eSight 网管系统可以针对第三方设备定制关于配置文件备份的备份、恢复、重启命令，支撑配置文件自动备份。

- 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。

11、 WLAN 网络管理

企业分支网络中的 AC，AP 部署分散，尤其 AP 数目众多，运维成本和难度大，为了能对 WLAN 网络中设备集中管理和对 WLAN 网络的可视化监控，eSight 产品提供 WLAN 管理组件解决这一运维难题 。



WLAN 网络管理特点：

- 简单快速的业务部署

向导式配置的业务部署以及基于表单 AP 导入，可加速 WLAN 的业务部署。通过对华为 AC 设备的管理，实现对 WLAN 业务的配置功能。AP 的信息都配置在 AC 上，当 AP 上线建立隧道后从 AC 获取信息。

- 业务拓扑和位置拓扑，方便用户对 WLAN 网络中设备进行可视化监控和集中管理

业务拓扑 ：展现 AC、AP、STA 之间连接关系查看，并示意 Rogue AP 的存在；支持 AP、AC、STA、Rogue AP 详细信息查看；并提供无线业务的故障诊断能力。

位置拓扑：查看当前热点位置及射频信号覆盖范围并在视图上标识当前非法 AP 位置及冲突域。颜色表示不同的频段， 深浅表示信号的范围，红色显示冲突域。

- AP 故障快速恢复能力，提供批量恢复 AP 的出厂设置、批量重启 AP 以及 AP 替换的功能。

AP 出现异常或在 WLAN 网络的调试过程中，用户可以通过网管远程批量恢复 AP 的出厂设置。

AP 升级完成后或在 WLAN 网络的调试过程中，用户可以通过网管远程批量重启 AP。

AP 出现硬件故障需要替换时，用户可以通过网管替换新 AP，快速保证 AP 替换后业务不变。

- 多样式资源统计，满足运维需求

全网资源统计：全网用户在线趋势图、TOP5 用户接入 Fit AP、TOP5 用户接入 SSID、TOP5 重点关注的设备告警列表、全网物理资源统计。

基于 AC 资源统计：根据 AC 统计用户在线趋势图、AP 信息、域信息、AC TOP5 告警。

基于 AP 资源统计：根据 AP 统计 TOP5 告警、当前 AP 性能 KPI（AP 关联终端数、AP 物理属性、AP 流量、射频流量等）。

基于 SSID 资源统计：根据 SSID 统计 AP、VAP、接入终端数。

基于区域与位置资源统计：根据区域与位置统计 AP 总数、AP 在线总数、STA 在线总线。

4 分支网络场景设计

4.1 微型分支场景

4.1.1 对应的细分市场

微型分支网络主要针对于接入点 10 个以下的场景，主要包括微型金融网点，移动银行网点/离行 ATM 机，微型连锁机构(加油站等)，小型餐饮连锁企业，SOHO 办公。

SOHO办公

微型金融机构

小型加油站

餐饮连锁

环境监测车

离行ATM机

微型金融网点的业务特点：

- 生产与办公业务隔离

- 银行要求可靠性高，E1/MSTP 或 E1/MSTP＋xDSL 双链路上行；证券要求稍低，MSTP 上行
- 有无线覆盖的需求，为员工和访客提供因特网接入
- 有语音接入需求

移动银行网点/离行 ATM 机的业务特点：

- 只有生产业务
- 可靠性要求不高。xDSL/3G 单链路上行
- 没有无线覆盖的的需求
- 无语音接入需求

微型连锁机构(加油站等)的业务特点：

- 生产与办公业务隔离
- 可靠性要求不高。xDSL/3G 单链路上行
- 没有无线覆盖需求
- 有语音接入需求

小型餐饮连锁企业的业务特点：

- 只有访客业务要求
- 可靠性要求不高。xDSL/3G/IP 专线单链路上行
- 有语音接入需求

SOHO 办公的业务特点：

- 只有办公业务要求
- 有无线覆盖需求
- 可靠性要求不高。xDSL/3G 单链路上行
- 有语音接入需求

4.1.2 网络设计要点

微型分支网络设计要点：

- 单设备 All in One 方案

  微型分支接入点数小于 10，业务简单，同时 IT 维护能力也弱，配备 AR150/200/1220 All in One 路由器可同时满足多种业务需求的前提下，减少设备数量，简化网络部署，方便客户运维。
- 单链路互联

  微型分支作为企业网络的末梢环节，数量众多，有与总部或地区部互通的需求，除非对可靠性要求极为苛刻的场景，否则考虑到费用的问题，一般选择单链路互联。互联的方式视具体情况而定，可选择拨号或专线接入。
- 网络扩展

对于诸如部署大量 IP 摄像头等设备的场合，会占用大量的 LAN 接口，可以考虑用二层交换机扩展接口。按照每摄像头 3M 流量算，不会影响到办公业务。

- 远程认证

  分支本地设备数量较少，IT 管理能力弱，只在出口部署认证点，分支内不部署认证服务器，另外从成本控制考虑也不适合部署服务器。

- 远程网管

  典型微型分支网络只有一台设备，无需本地网管。从企业运行成本控制考虑，在总部或地区部部署网管设备，从而对分支设备进行统一有序的远程管理，减少维护工作量和出差费用。

4.1.3 方案设计

针对微型分支网络的业务特点，华为融易分支微型分支网络的整体拓扑图如下。

设计方案总体特点：

- 上行链路互联：

  当选择单链路上行时，可以选择传输专线/xDSL/3G/xPON，对于安全性/可靠性要求极高场合，也可选择双链路上行。

- 视频监控：

  提供 POE 供电，简化布线。IT 网络提供融合 IP 视频监控

- 语音：

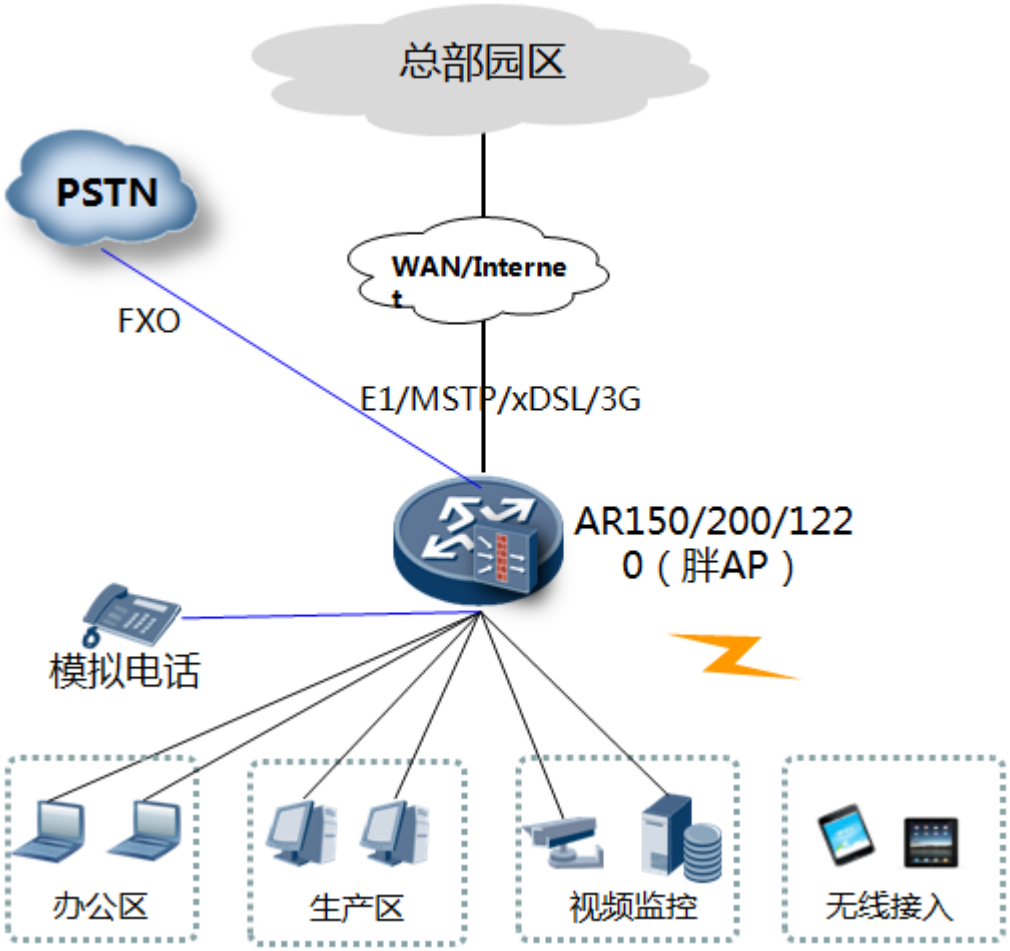
  同时支持模拟和 IP 话机，提供支持 IP PBX 模式、AG 模式

- 安全：

  提供集成防火墙功能，IPSec 硬件加密隧道

- 网管：

  总部部署网管，分支统一管理



微型分支无线部署（免认证方式）

微型分支无线接入（免认证方式）特点：

- 无线接入

  建议采用 AR151W/AR1220W 款型集成胖 AP 的一体化接入路由器，来满足微型分支场景的无线覆盖的要求。

  管理主机通过以太口连接到路由器，起到管理作用。

- 内部员工/访客隔离

  AR 分别为内部员工和访客配置不同 SSID，两者之间二层隔离。

  两类用户都通过 WLAN 接入 Internet。

  访客与内网之间无路由可达，保证内网安全。

微型分支无线部署（需认证方式）

微型分支无线接入（需认证方式）特点：

- 无线接入

  建议采用 AR1220W 款型集成胖 AP 的一体化接入路由器，来满足微型分支场景的无线覆盖的要求

- 内部员工/访客隔离

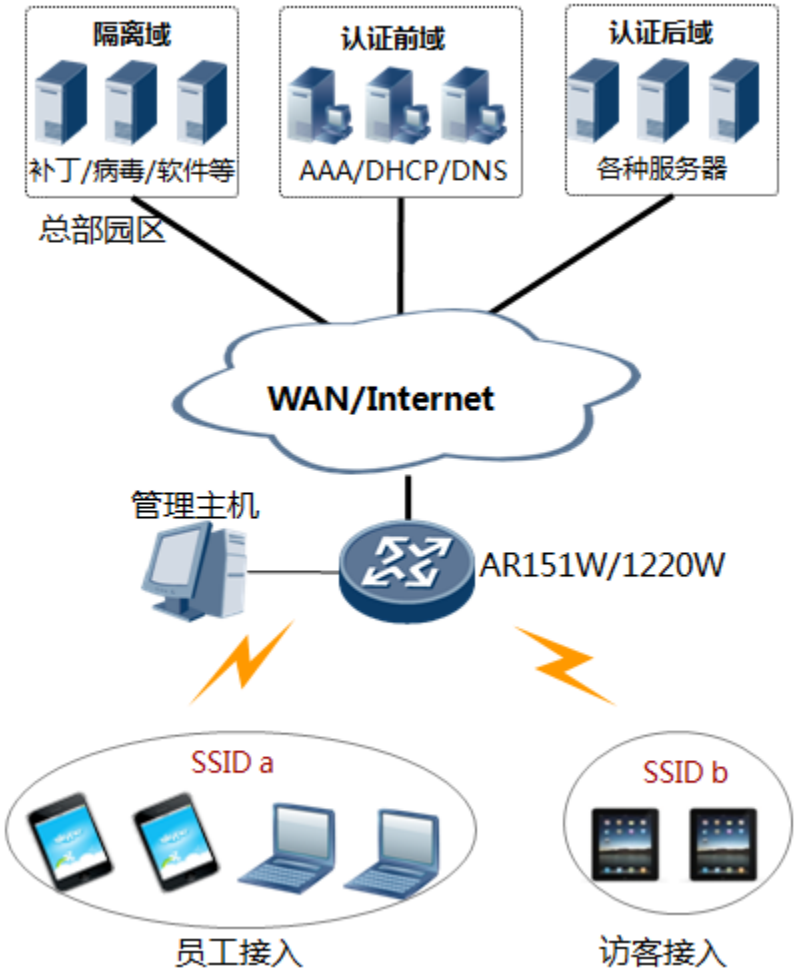
  AR 分别为内部员工和外部访客配置不同 SSID，分别对应不同子网，便于访问权限策略控制。

  开放内部员工访问内部网权限。开放访客子网到因特网权限。

- 安全认证

  对内部员工选择采用 802.1x 或 Portal 认证方式;对访客采用 Portal 认证方式。802.1x 安全性高，适合内部员工；Portal 认证不需安装客户端，适合访客。

  接入控制点/授权控制点均位于 AR。认证/授权/计费等服务器、隔离域服务器、认证后域服务器在总部。



终端认证方式

终端认证方式的选择：

- 哑终端(包括 IP 电话机、打印机、传真机等)采用 MAC 认证
- 生产用机(有线接入) 采用 802.1x 认证
- 办公用机(有线接入) 采用 802.1x 认证
- 办公用机(便携机无线接入、pad、智能手机等) 采用 Portal 认证
- 访客终端(无线接入) 采用 Portal 认证

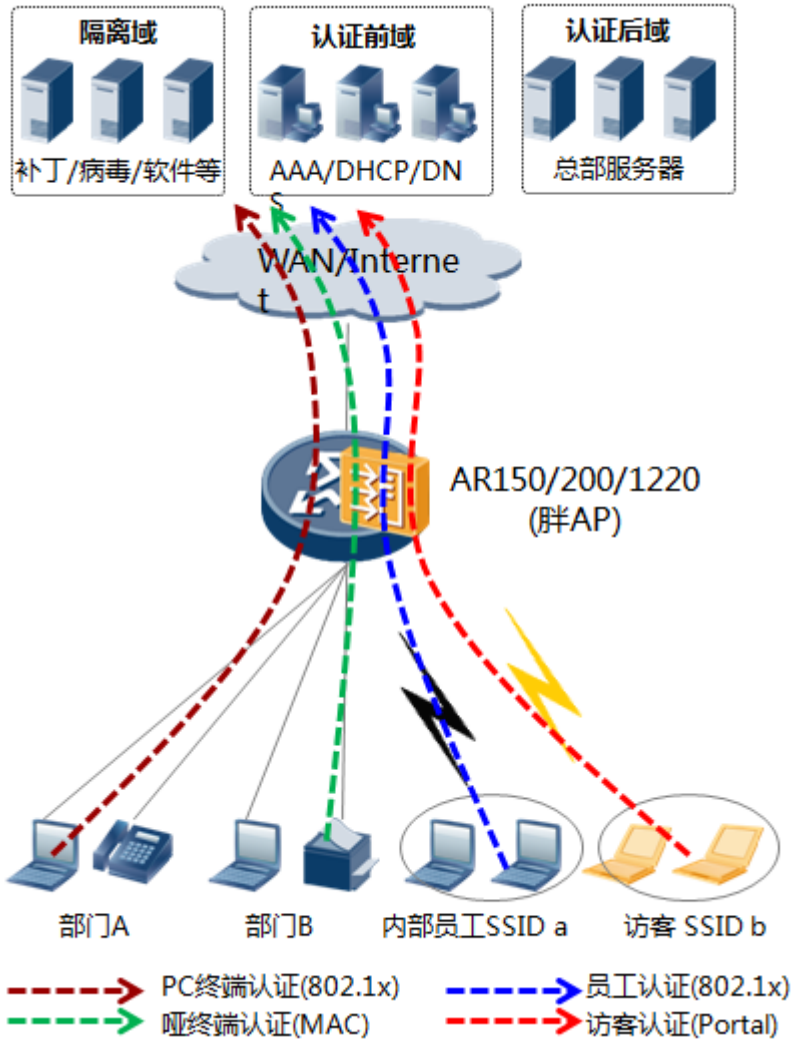
终端接入控制部署

终端接入控制部署的方式：

- 出口路由器作为所有认证方式的接入控制点
- 微型分支不适合部署认证/授权服务器，因此认证/授权服务器部署在总部
- 有线用户：出口路由器启用 802.1X＋MAC 自适应认证
- 无线用户：企业员工访问接入点与访客接入点不同，分别在 AC 启用 802.1X 认证和 Portal 认证。员工的无线终端通过 802.1X 认证接入分支，访客无线终端通过 Portal 认证接入分支
- IP 电话、IP 摄像头、打印机等哑终端采用 MAC 认证

客户价值：

- AR 路由器支持全面的认证方式，不同认证方式适应多种场合的接入，保障分支网络安全
- AR 集成接入 LAN 口、出口路由器与胖 AP 功能。



微型分支安全部署

微型分支无线安全部署特点：

- AR 集成防火墙功能

  AR 集成防火墙，支持划分安全域，可实现内/外网络间隔离。

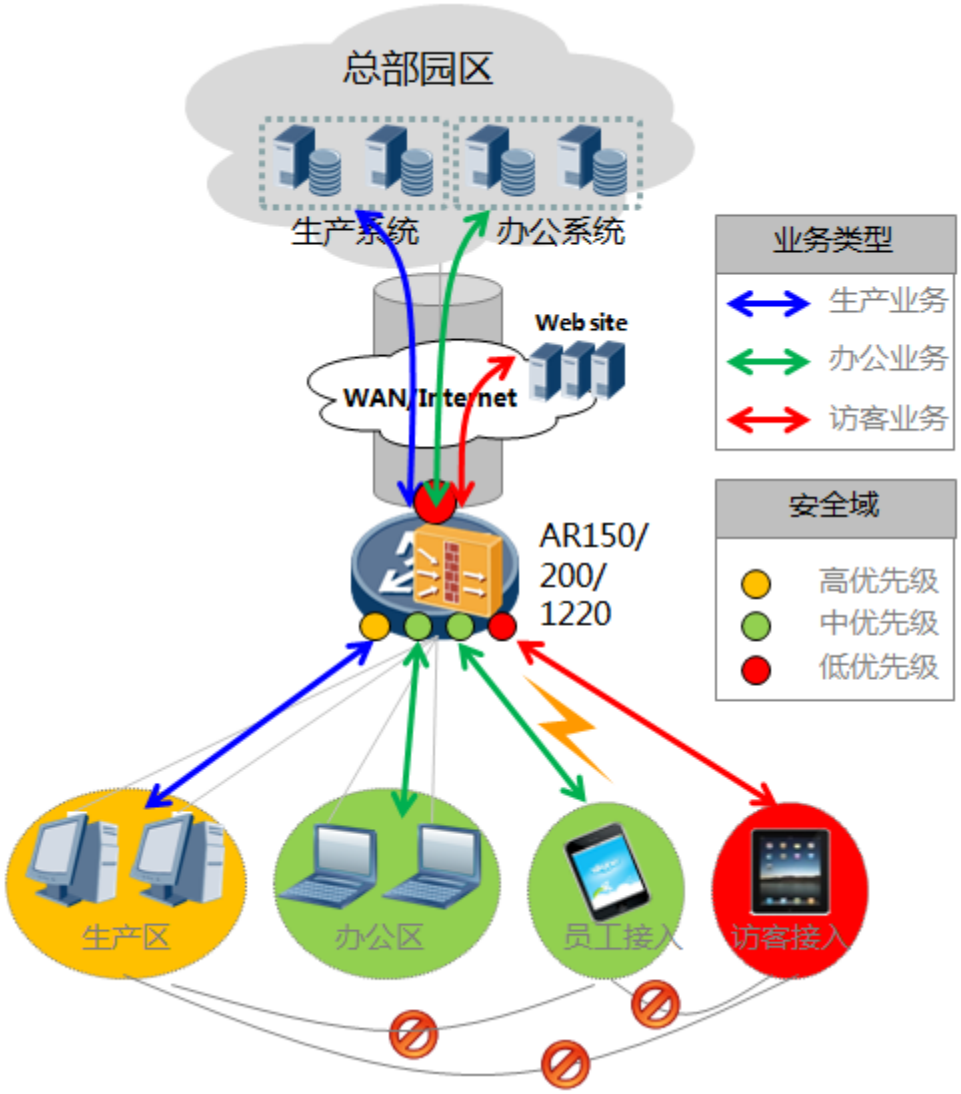
- 安全域隔离

  生产区/办公区归属不同 vlan，对应的 vlanif 加入相应安全域。

  内部员工/访客无线接入不同 SSID，对应不同 vlan，对应 vlanif 加入相应安全域。内部员工优先级可与办公区相同或者低，但比访客区高。

  访客安全域等级与路由器出口相同，只能访问 Internet。

  路由器出口为最低安全域等级，禁止外网发起的访问。



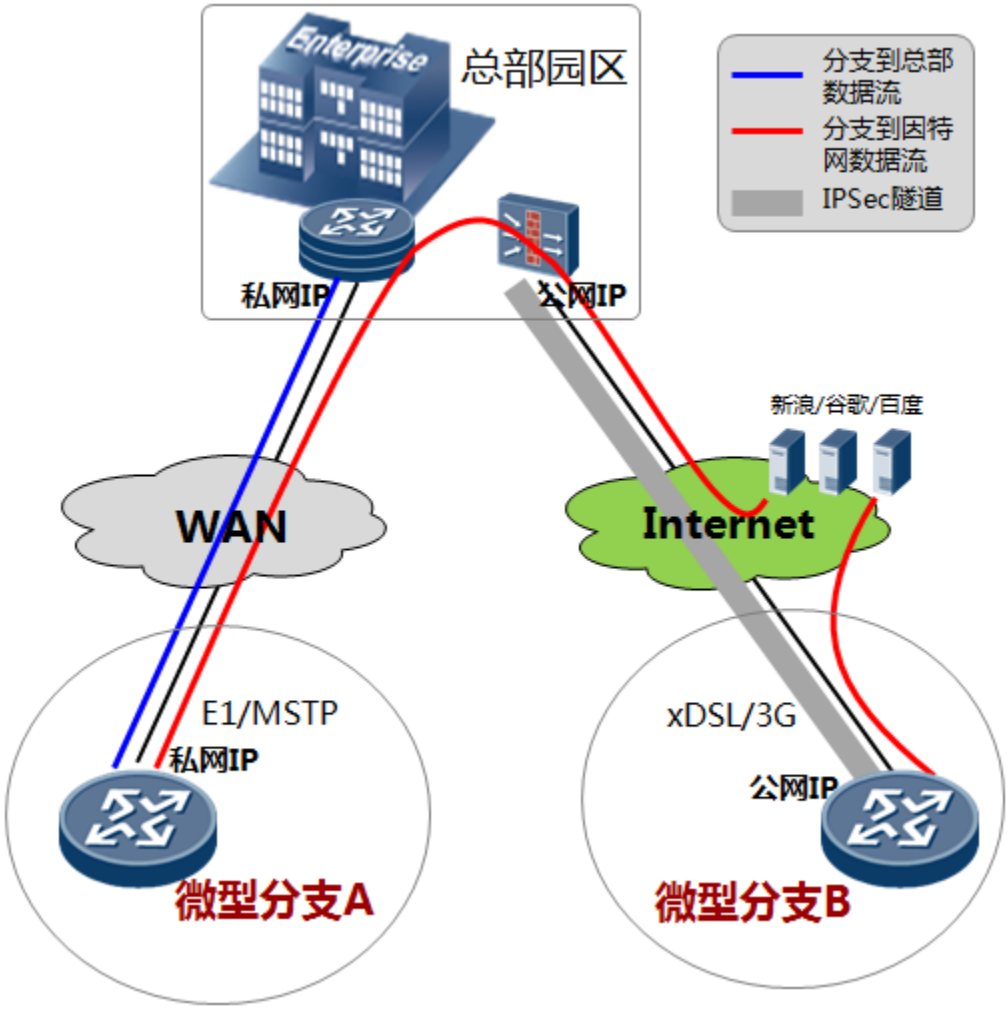
微型分支与总部互联方式

Internet 互联方式：

- 分支通过 xDSL/3G 链路拨号上网，分支与总部的互访通过建立在 AR 与 VPN 之间的 IPSec 隧道，分支上网流量通过 AR 路由器 NAT 穿越实现
- 此方式对可靠性/安全性要求一般，各分支有上网需求和互联需求的场景适合此种方式。分支根据具体情况选择上网方式：3G/xDSL/IP 专线/xPON 等

WAN 互联方式：

- 分支通过 E1/MSTP 等链路，与总部之间通过 WAN 连接
- 分支直接访问总部园区网络
- 分支上网流量通过总部的网关设备
- 此方式对可靠性/安全性要求高，企业采用统一互联网出口的场景适合用 WAN 互联。



微型分支与总部互联方式（Internet 互联）

分支网络部署：

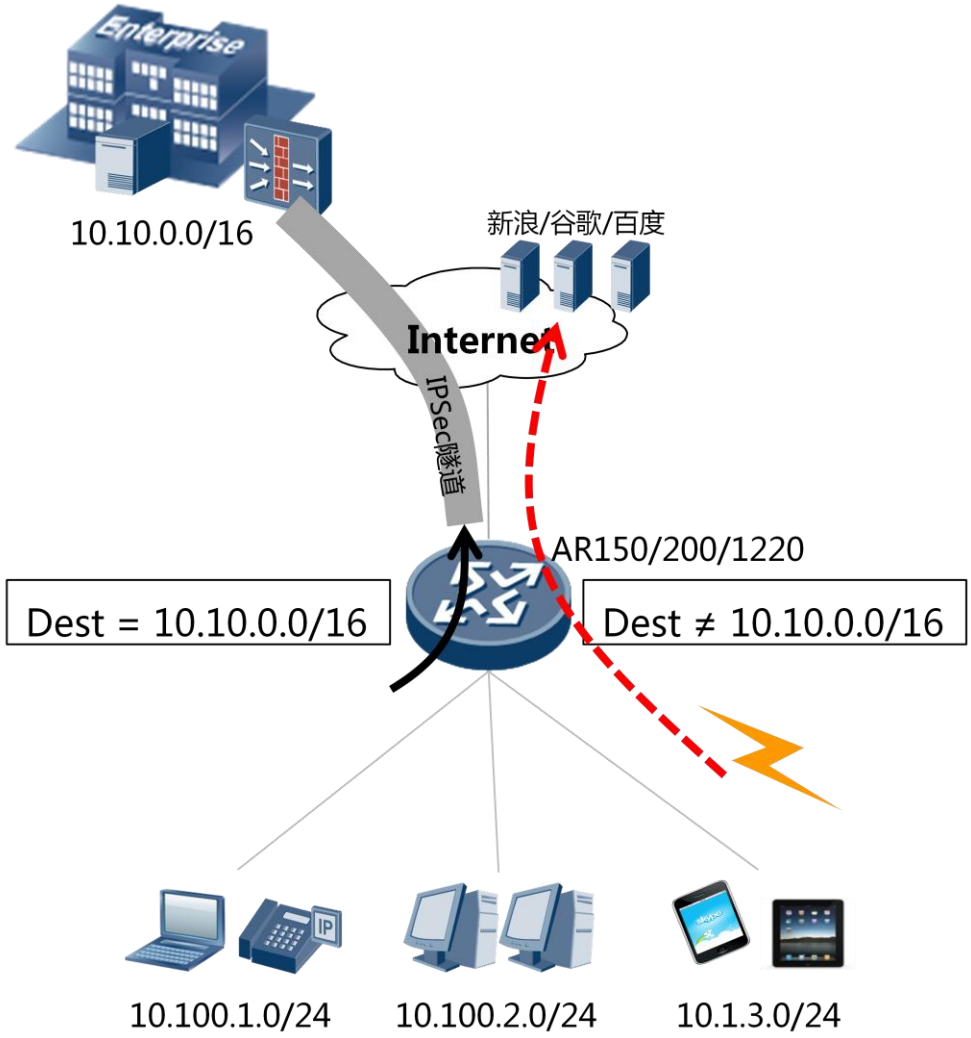
- AR 拨号后生成到因特网的缺省路由，所有报文通过该路由出分支
- 目的地为企业总部的数据，匹配 ACL，进 IPSec 隧道，安全到达总部
- 到因特网的数据，经 NAT 地址转换后，直接访问因特网服务器

总部网络部署：

- 总部部署 VPN 网关，接收分支的 IPSec 连接
- 应用专线连接因特网，采用静态公网 IP 地址

互联特点：

- 对可靠性/安全性要求一般，各分支有上网需求和互联需求的场景适合此种方式。
- 分支根据具体情况选择上网方式：3G/xDSL/IP 专线/xPON 等

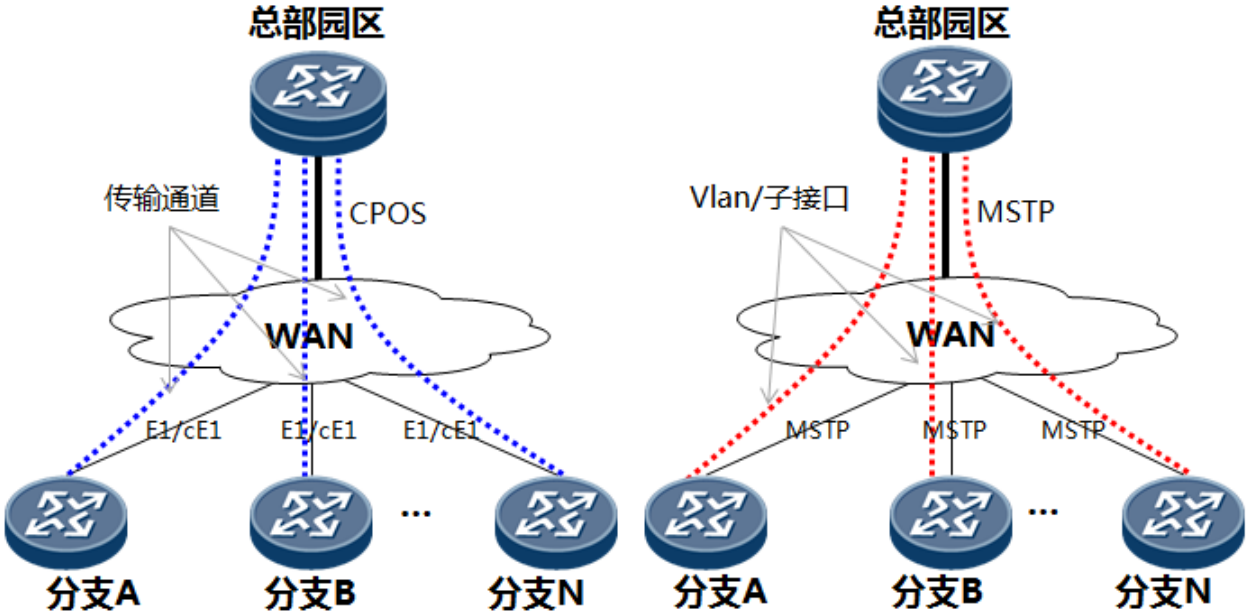


微型分支与总部互联方式（WAN 互联）

采用的链路方式：

- 分支通过通道化 E1 连接到 WAN，总部通过 CPOS 连接到 WAN。构成物理上的点对多点的拓扑。CPOS 的每个通道对应每个分支的通道化 E1，构成分支与总部间点对点拓扑。

- 分支与总部分别通过 MSTP 连接到 WAN，物理拓扑上属于点对多点的结构。对于二层口连接，总部 MSTP 通过不同 VLAN 对接分支的 MSTP 接口，形成逻辑上的点对点连接。对于三层口连接，总部 MSTP 通过子接口与各分支形成逻辑点对点连接。



采用的路由方式：

- 静态路由方式适合分支数量少的情况，AR 配置缺省路由，下一跳出口为分支 E1/MSTP 链路出口，与分支相对的总部路由器配置到各个分支网络的静态路由

- 动态路由协议适合分支数量大，采用静态路由配置起来比较繁琐的情况，动态路由协议通常采用 RIP 或 OSPF。

互联特点：

- 对可靠性/安全性要求高，企业采用统一互联网出口的场景适合用 WAN 互联。

微型分支语音部署

微型分支运维部署特点：

- 适用场景

  微型分支规模终端接入点在 10 以内，语音终端接入号码数小于 10。

  典型场景如加油站、SOHO 办公、微型金融机构等。

- 分支部署

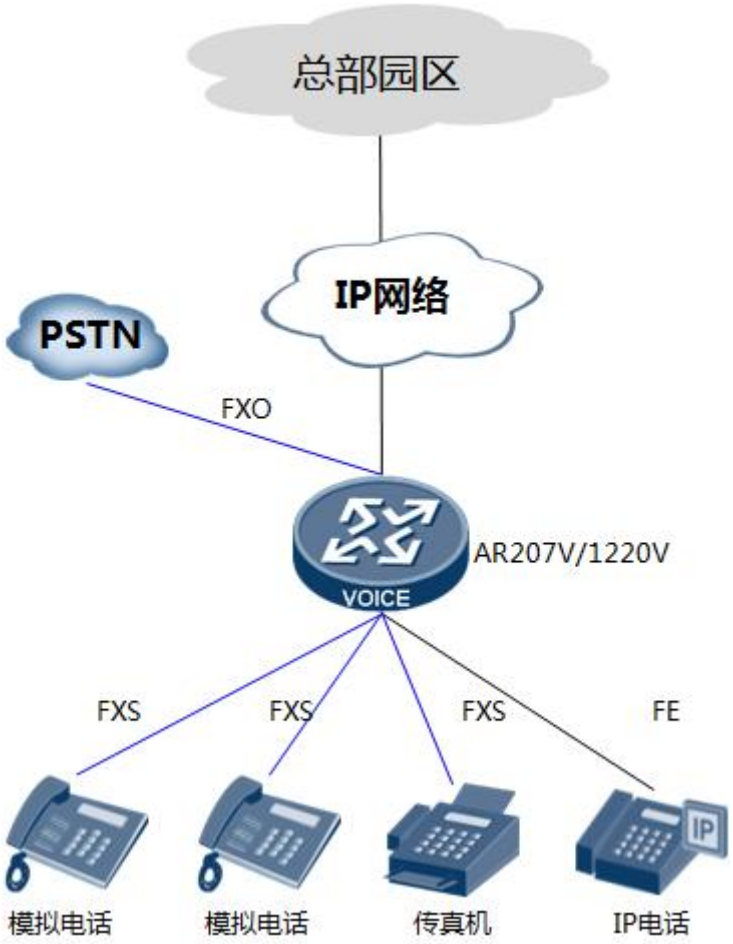
  AR 配置语音功能，可选择部署 SIP-PBX 或者 SIP-AG 模式。

  SIP PBX 部署模式下，可以开启更多语音功能，如 IVR 功能。并可充分享受总部园区已有的语音补充业务，如电话会议功能。

  AR 通过 1 个或多个 FXO 接口接入 PSTN，可同时多路跟外线互通。

- 客户价值

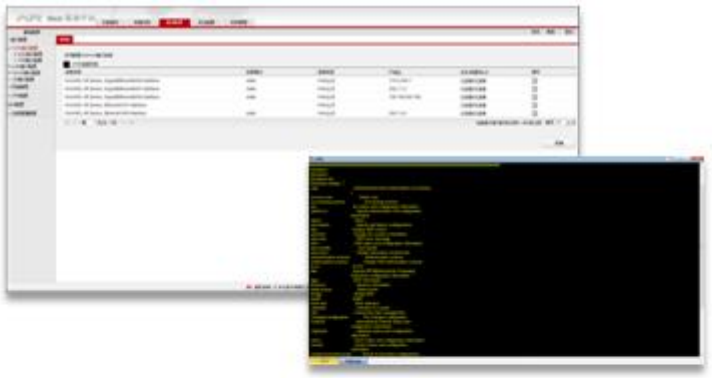
  AR 语音、数据统一，减少网络布线，快速组建网络，节省投资成本。



微型分支运维部署

微型分支运维部署特点：

- 本地单设备管理
  使用 CLI 管理方式。
  通过 console 口、MiniUSB 进行本地管理。
  通过 Telnet、SSH 进行本地管理。
- WEB 管理方式
  通过 web 页面对设备进行配置管理



- 远程分支统一管理
  总部部署 eSight，自动发现分支设备并远程统一管理。
  总部也可通过 Telnet/SSH 远程对分支管理。
  总部安装 IPSec VPN、WLAN 等组件，实施增值业务管理。

4.1.4 典型配置建议（推荐产品、板卡）

微型分支产品推荐如下图：

规格/产品型号	AR150	AR200	AR1200
基础转发性能	300kpps	450kpps	450kpps
固定LAN口	4×FE电口	8×FE电口	8×FE电口
固定WAN口	AR151：1×电口FE AR157：1×ADSL	AR201：1×电口FE AR206/7/8：1×xDSL AR207G：内置1×3G	2×GE电口
支持插槽数	0	0	2×SIC插槽/1×WSIC插槽
备注	1）不支持插槽，两款子型号151/157差别在固定WAN口 2）AR151W支持Wifi 3）无支持3G的型号 4）无支持话音的型号	1）只有固定口，不支持插槽。 2）无支持Wifi的型号 3）207V支持8路语音 4）AR206/7/8的主要区别在支持的xDSL类型不同	1）支持2×SIC或1×WSIC 2）AR1220V支持IP语音 3）AR1220W支持Wifi 4）AR1220VW同时支持语音Wifi 5）支持插2块×3G SIC卡，形成3G主备链路上行

微型分支典型场景&产品选型如下图：

场景(微型)	需求	推荐产品	备注
微型金融网点	双E1+WLAN；语音	AR1220VW+2*E1 SIC卡+4FXS1FXO卡（1块）	1）AR200都不支持E1 2）AR200中除AR207G之外都不支持3G 3）AR200都不支持SIC卡 4）AR1220支持2SIC 5）常用SIC卡的类型： 4FXS＋1FXO 1 E1 2 E1 1 xDSL 2 xPON（GPON＋EPON） 1 HSPA＋7卡 1 GE Combo 1 cPOS WAN 6）常用WSIC卡的类型： 8FE＋1GE 2 CE1 2 FE WAN 语音单板除了4FXS+1FXO外，其它的没列 ·若模拟语音，需搭配4S1O卡 AR207有专门分销市场版本：AR207-S。
	双MSTP+WLAN；语音	AR1220VW+4FXS1FXO卡（2块）	
	E1+3G/xDSL+WLAN；语音	AR1220VW+1*E1 SIC卡+USB 3GUSB或SIC卡/xDSL SIC卡。注：对于E1+xDSL和E1+3G SIC方案，无法支持模拟语音接入	
	xDSL+3G+WLAN；语音	AR1220VW+xDSL SIC卡+USB 3G卡/3G SIC卡。若选用3G SIC卡则不支持模拟语音接入	
移动金融网点/离行ATM	单3G	AR207G	
	双3G	AR1220+双USB 3G卡 或 AR1220+USB 3G卡+3G SIC卡	
连锁机构(加油站等)	3G/xDSL	AR207G；AR207	
	3G/xDSL+WLAN	AR1220W+USB 3G卡/3G SIC卡，AR1220W+xDSL SIC卡。或者AR207G+AP，AR207+AP	
	3G/xDSL+WLAN；语音	AR1220VW+3G USB卡/3G SIC卡+4FXS1FXO，AR1220VW+xDSL SIC卡+4FXS1FXO。	
餐饮连锁	3G/xDSL/以太专线＋WLAN	AR1220W+3G USB卡/3G SIC卡；AR1220W+xDSL SIC卡；AR1220W	
SOHO办公	xDSL+WLAN；语音	AR157+AP（不支持语音）；AR1220W+xDSL SIC卡+4FXS1FXO	

4.2 小型分支场景

4.2.1 对应的细分市场

小型分支网络主要针对于接入点 10 到 50 个场景，主要包括小型银行网点，证券营业网点，小型税务，连锁超市，小企业的分支机构等。

小型银行网点

证券营业网点

小型税务

连锁超市

小企业分支

小型银行网点的业务特点：

- 生产/办公隔离
- 本地不部署业务服务器
- 银行要求可靠性高，推荐出口双 E1/MSTP 或 E1/MSTP＋xDSL，连接到上级机构
- 有无线覆盖的需求，为员工和访客提供因特网接入

证券营业网点的业务特点：

- 新型的证券网点只有办公业务，新型网点已经没有交易业务

- 本地不部署业务服务器
- 可靠性要求高，双 E1/MSTP 出口，直接连接到券商总部或数据中心

小企业的分支机构的业务特点：

- 业务部门间需要隔离
- 本地不部署业务服务器
- 有无线覆盖需求
- 可靠性要求各不相同，可以采用 xDSL/3G/xPON/E1/MSTP 等多种方式上联

4.2.2 网络设计要点

小型分支网络设计要点：

- 单核心设备 All in One，外围设备扩展接入点

  小型分支接入点数小于 50，业务简单但部门稍多，地域比微型分支稍广。配备单核心，视业务需求采用 AR200 或 1220 All in One 路由器，二层交换级扩展有线接入、瘦 AP 扩展无线接入。

- 单或双链路互联

  可靠性要求高的场合选择双链路上行，否则选择单链路，节省费用。若采用主备链路，主链路视业务对可靠性和带宽需求，可选择企业专线、拨号、IP 专线或 xPON；备链路可用 3G，流量计费，费用最省。

- 远程认证

  分支本地设备数量较少，IT 管理能力弱，只在出口部署认证点，分支内不部署认证服务器，另外从成本控制考虑也不适合部署服务器。

- 远程网管

  小型分支网络只有数台设备，无需本地网管。从企业运行成本控制考虑，在总部或地区部部署网管设备，从而对分支设备进行统一有序的远程管理，减少维护工作量和出差费用。

4.2.3 方案设计

针对小型分支网络的业务特点，华为融易分支小型分支网络的整体拓扑图如下。

设计方案总体特点：

- 上行链路互联：

  对可靠性/安全性要求高的场景，可以选择负载分担或主备链路的双链路上行方式

  对可靠性要求一版的场景，可以视业务需求选择不同的单链路上行连接方式

- 语音：

  同时支持模拟和 IP 话机，提供支持 IP PBX 模式、AG 模式

- 安全：

  提供集成防火墙功能，IPSec 硬件加密隧道，提供安全区域隔离不同业务子网和内外网

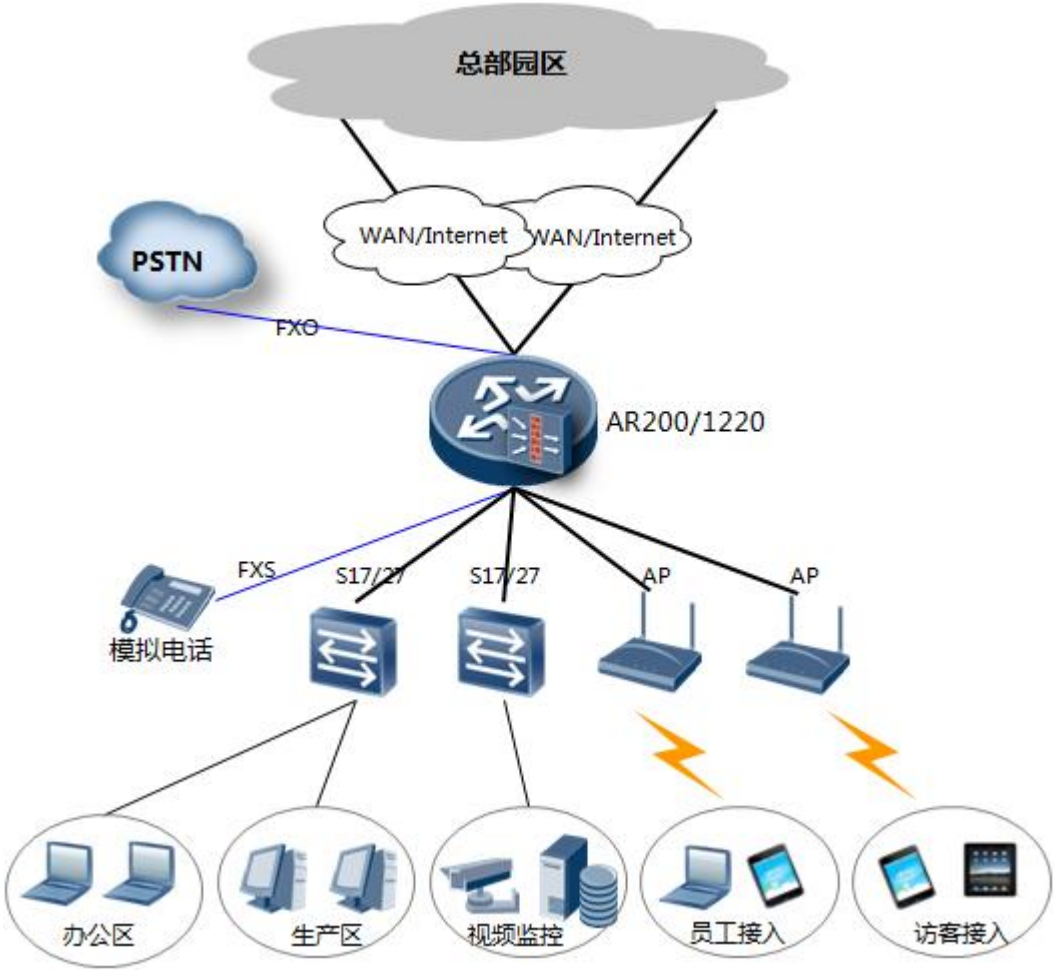
- 二层接入/子网隔离

  接入交换机扩充端口，支持划分 vlan，实现灵活的二层隔离

  AP 满足无线用户的接入，内外用户设置不同 SSID

- 网管：

  总部部署网管，分支统一管理



小型分支无线部署

微型分支无线接入特点：

- 无线设备

建议 AP 采用华为接入点设备，接入控制器采用 AR 集成，可以节省投资。

- 内部员工/访客隔离

  AR 分别为内部员工和外部访客配置不同 SSID，分别对应不同子网，便于访问权限策略控制。

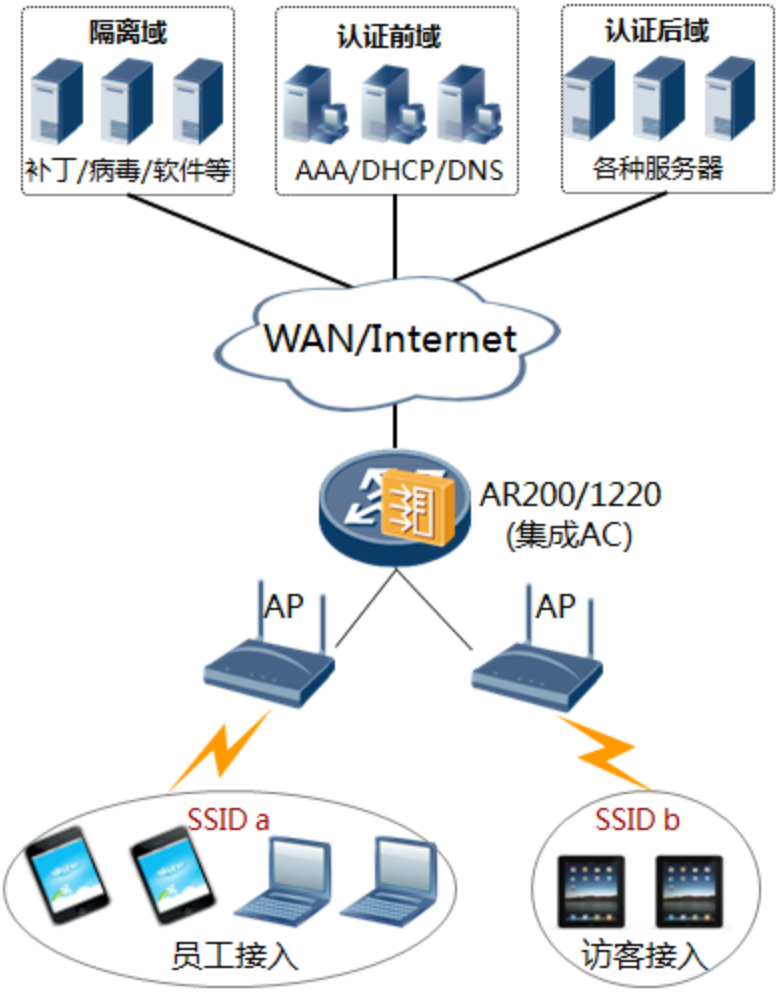
  开放内部员工访问内部网权限。开放访客子网到因特网权限。

- 安全认证

  对内部员工选择采用 802.1x 或 Portal 认证方式;对访客采用 Portal 认证方式。802.1x 安全性高，适合内部员工；Portal 认证不需安装客户端，适合访客。

  有线终端接入认证点/授权控制点均位于 AR；无线终端接入认证点位于集成的 AC，控制点位于 AP。

  认证/授权/计费等服务器、隔离域服务器、认证后域服务器在总部。



终端认证方式

终端认证方式的选择：

- 哑终端(包括 IP 电话机、打印机、传真机等)采用 MAC 认证
- 生产用机(有线接入) 采用 802.1x 认证
- 办公用机(有线接入) 采用 802.1x 认证
- 办公用机(便携机无线接入、pad、智能手机等) 采用 Portal 认证
- 访客终端(无线接入) 采用 Portal 认证

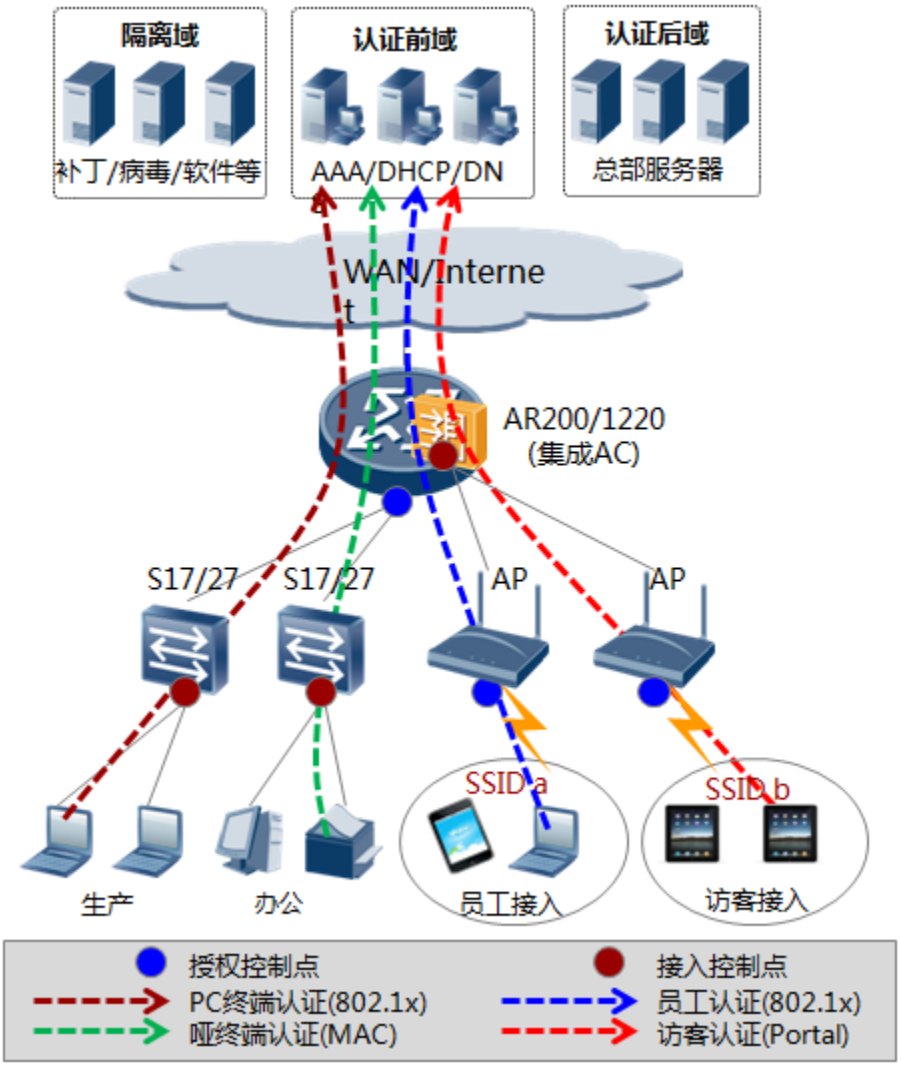
终端接入控制部署

终端接入控制部署的方式：

- 小型分支不适合部署认证/授权服务器，认证/授权服务器部署在总部
- 对于有线用户：接入/授权控制点分别在接入交换机和 AR 路由器。AR 路由器启用 802.1X＋MAC 自适应认证，分别对应 PC 和哑终端。
- 对于无线用户：接入点和控制点分别在集成 AC 和 AP。企业员工采用 802.1X 认证，访客采用 Portal 认证。

客户价值：

- 员工无线接入采用更安全的 802.1x 认证
- 访客无线接入采用更灵活的 Portal 认证，方便接入



小型分支安全部署

微型分支无线安全部署特点：

- AR 集成防火墙功能

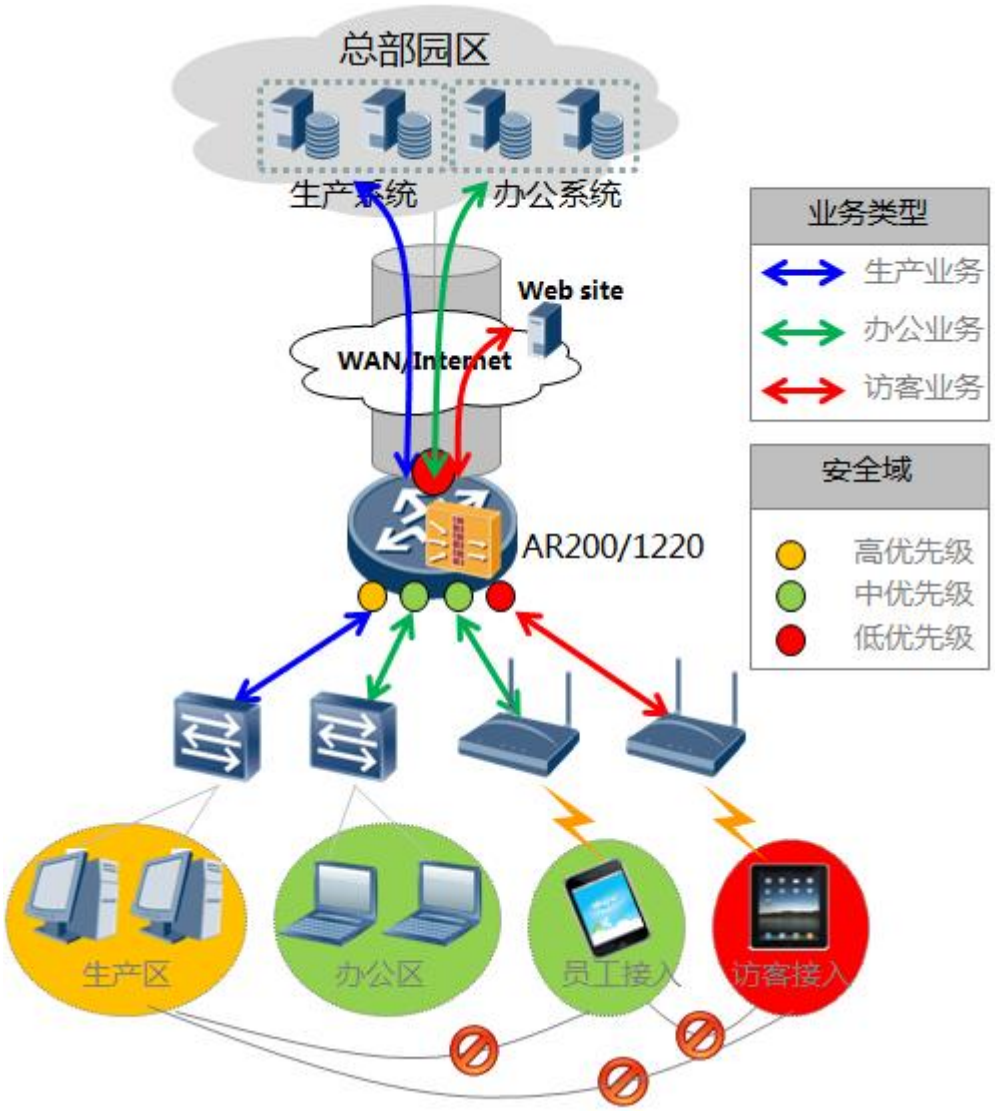
  支持划分安全域，可实现内/外网络间隔离，但不支持 IPS 和 anti-DDos
- 安全隔离(安全域)

  生产区/办公区划归不同 VLAN，对应的 vlanif 加入相应安全域。

  内部员工/访客无线接入不同 SSID，对应不同 vlan，对应 vlanif 加入相应安全域。内部员工优先级可与办公区相同或者低，但比访客区高。

访客安全域等级与路由器出口相同，只能访问 Internet。

路由器出口最低安全域等级，禁止外网发起的访问。



小型分支与总部互联方式

小型分支与总部互联方式：

- 单链路 Internet 互联

  对可靠性/安全性要求一般，同时有上网需求和互联需求的小型分支可采用此种互联方式。具体的互联方式视需求可选择 3G/xDSL/IP 专线/xPON 等。

- 单链路 WAN 互联

某些对可靠性要求高，或者对上网安全性要求高的行业，可以考虑分支与总部间WAN 互联。WAN 互联方式保证分支与总部间通路的可靠性和私密性；总部部署全网统一的互联网出口、统一的安全防护，确保了整网的边界安全。

- 双链路互联

  双链路互联是比 WAN 互联更为可靠的双保险方式。双链路可以是 WAN+WAN 或者 WAN+Ineternet。前者通常工作在源地址路由方式对流量进行规划，以隔离生产和办公业务；后者通常为主备方式：WAN 链路走内部互联业务，Internet 链路走上网流量，并作为 WAN 链路的备份。该方案适用于极高可靠性和用户对费用不敏感的场景。

单链路 Internet 互联

适用场景：

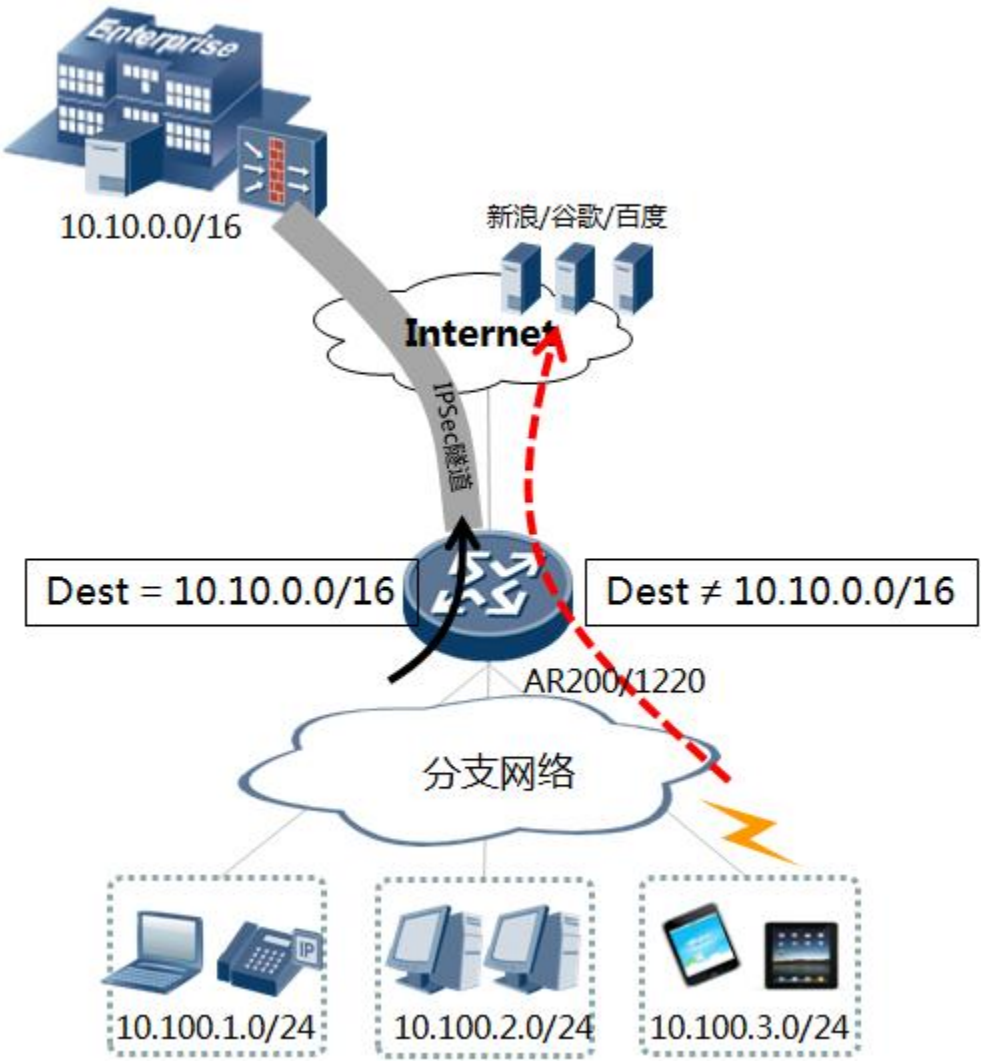
- 对可靠性/安全性要求一般，同时有上网需求和互联需求的小型分支可采用此种互联方式。具体的互联方式视需求选择 3G/xDSL/IP 专线/xPON 等

总部园区部署：

- 总部部署 VPN 网关，接收分支的 IPSec 连接
- 应用专线连接因特网，采用静态公网 IP 地址

分支网络部署：

- AR 拨号后生成到因特网的缺省路由，所有报文通过该路由出分支。
- 目的地为企业总部的数据，匹配 ACL，进 IPSec 隧道，安全到达总部。
- 到因特网的数据，经 NAT 地址转换后，直接访问因特网服务器

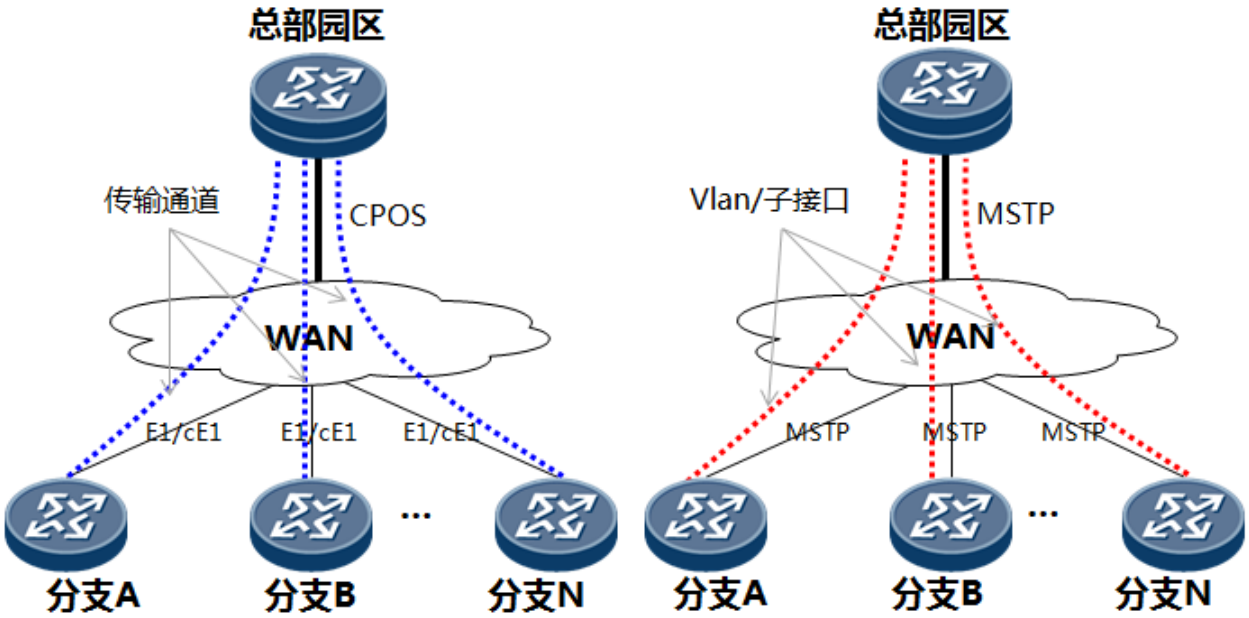


单链路 WAN 互联

采用的链路方式：

- 分支通过通道化 E1 连接到 WAN，总部通过 CPOS 连接到 WAN。构成物理上的点对多点的拓扑。CPOS 的每个通道对应每个分支的通道化 E1，构成分支与总部间点对点拓扑。

- 分支与总部分别通过 MSTP 连接到 WAN，物理拓扑上属于点对多点的结构。对于二层口连接，总部 MSTP 通过不同 VLAN 对接分支的 MSTP 接口，形成逻辑上的点对点连接。对于三层口连接，总部 MSTP 通过子接口与各分支形成逻辑点对点连接。



采用的路由方式：

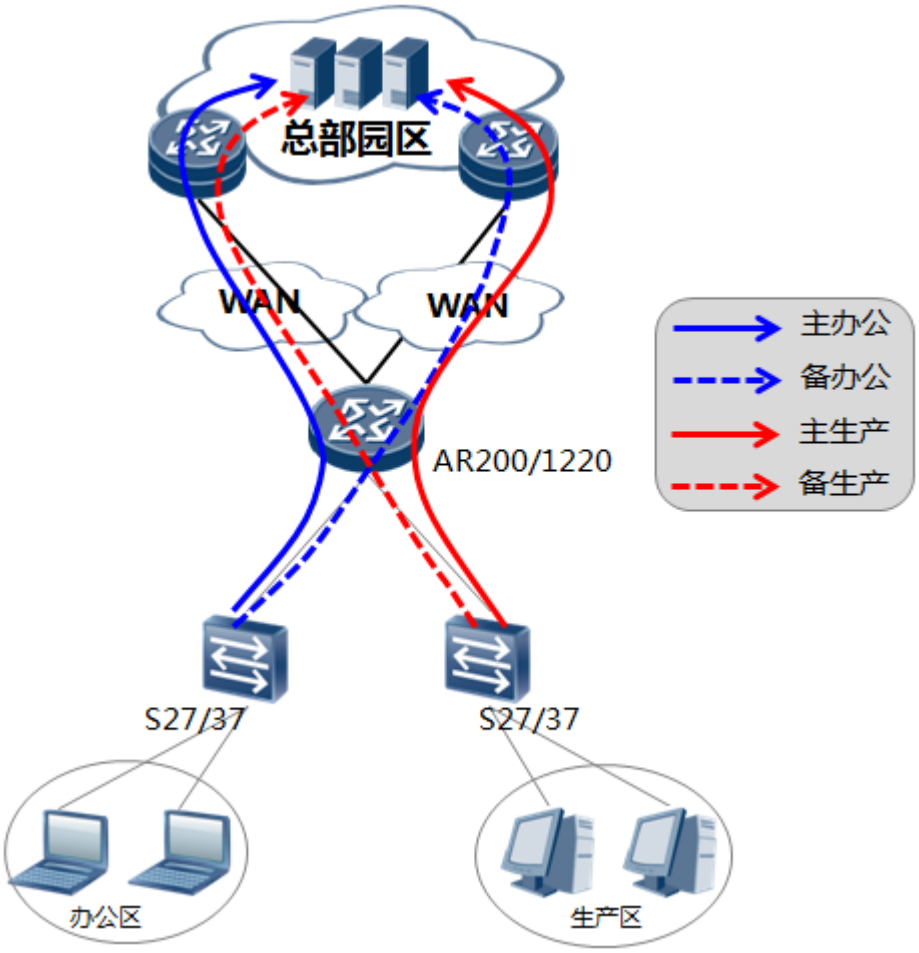
- 静态路由方式适合分支数量少的情况，AR 配置缺省路由，下一跳出口为分支 E1/MSTP 链路出口，与分支相对的总部路由器配置到各个分支网络的静态路由

- 动态路由协议适合分支数量大，采用静态路由配置起来比较繁琐的情况，动态路由协议通常采用 RIP 或 OSPF。

双 WAN 链路互联

互联特点：

- 出口路由器 AR200/1220 使用双 WAN 链路上行到总部：采用 E1/MSTP/MPLS 专线等方式。两链路互为备份，配置 BFD 快速检测，任一链路 down 后，业务能够及时切换到另一条链路。
- AR 路由器执行源地址路由，将生产/办公业务分配到不同 WAN 链路，实现业务隔离。

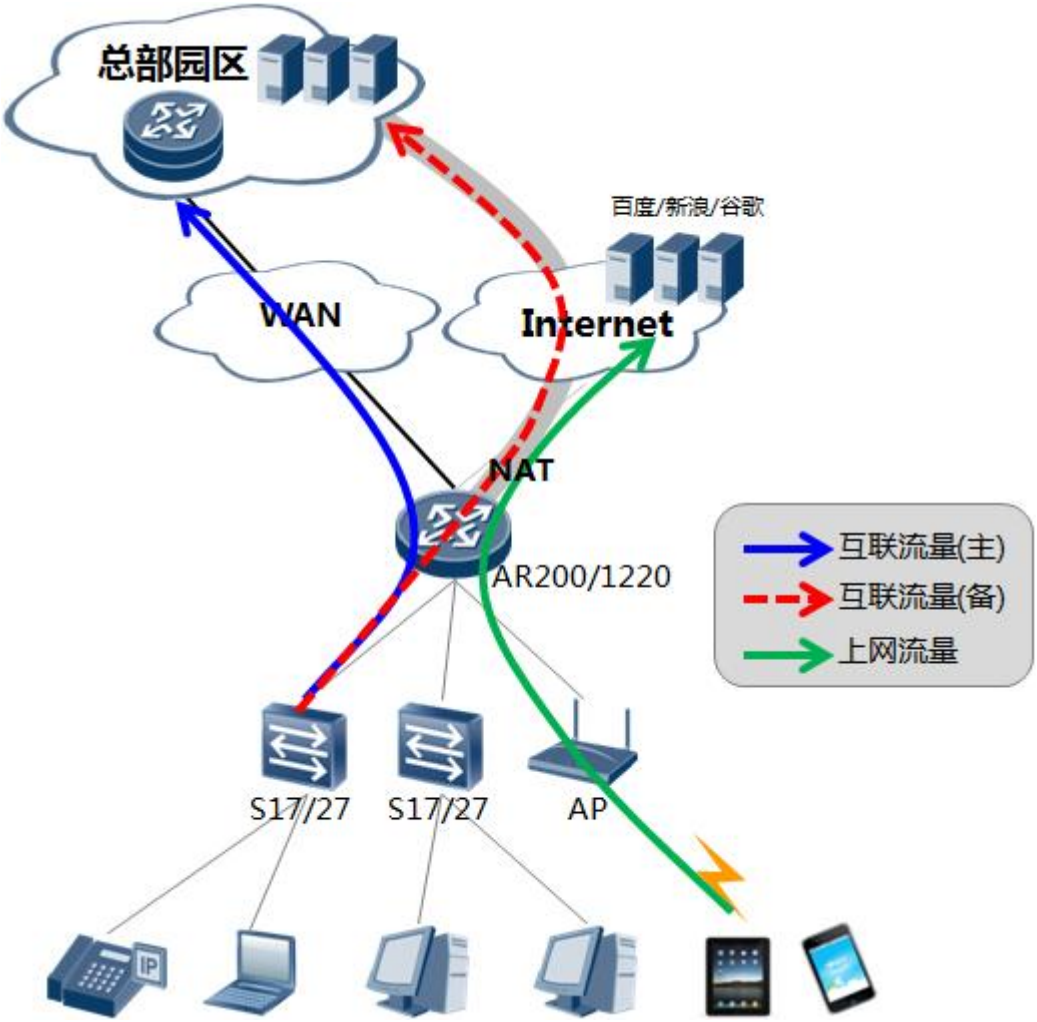


双 WAN 链路互联

互联特点：

- WAN 链路采用 E1/MSTP/MPLS 专线，作为分支与总部互联的主链路。Internet 链路采用 3G/xDSL/IP 专线/xPON 等。用于接入因特网，为分支提供上网服务；同时建立起在其上的 IPSec 隧道作为分支/总部互联的备份链路。
- WAN 链路两端运行动态路由协议或者静态路由，为加速路由收敛，可配置 BFD。

- AR 路由器配置经过 Internet 隧道的静态路由，其优先级要低于通过动态协议学习到的路由。WAN 链路正常时不走流量，WAN 链路 Down 后，流量经 IPSec 隧道抵达总部。



小型分支语音部署

小型分支运维部署特点：

- 适用场景

  小型分支规模终端接入点在 10~50 左右，语音终端接入号码数小于 30。

  典型场景如连锁超市、小型企业分支、证券营业网点等。

- 分支部署

  AR 配置语音功能，可选择部署 SIP-PBX 或者 SIP-AG 模式。

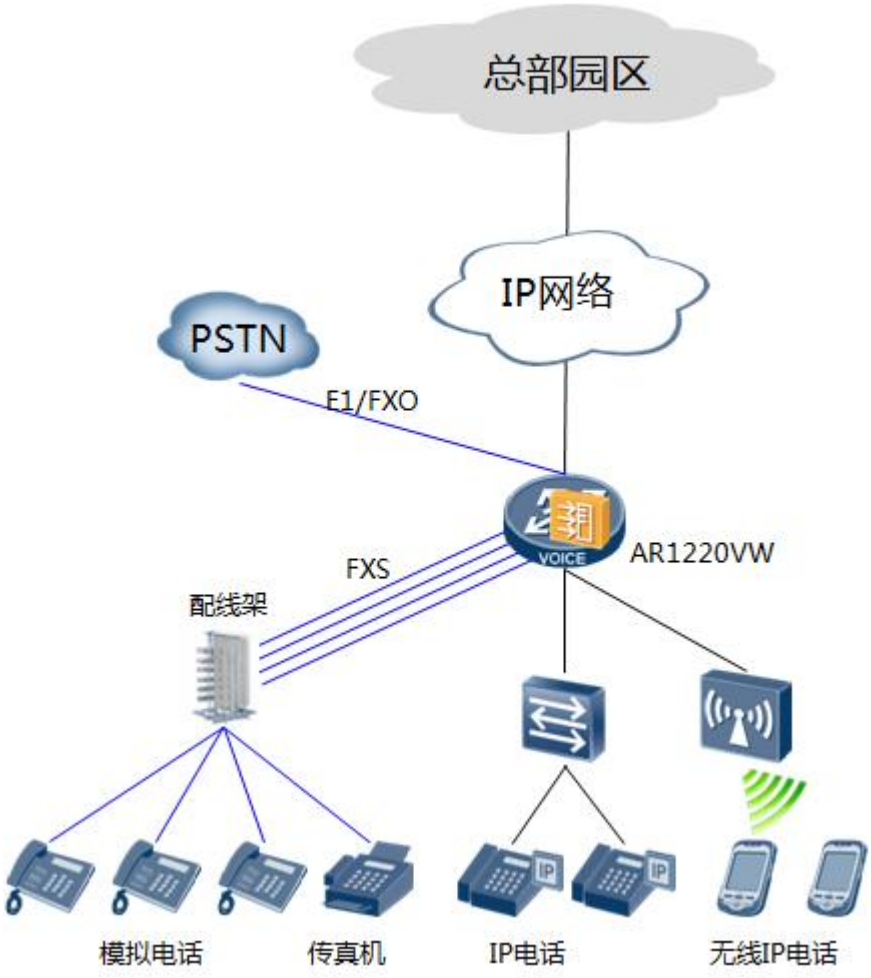
  SIP PBX 部署模式下，可以开启更多语音功能，如 IVR 功能。并可充分享受总部园区已有的语音补充业务，如电话会议功能。

  AR 集成胖 AP 或者 AR 集成 AC+瘦 AP 提供无线 IP 电话的 WIFI 接入。

  AR 通过 1 个或多个 FXO 接口接入 PSTN，可同时多路跟外线互通。

- 客户价值

  AR 语音、WLAN 统一，支持模拟电话、有线、无线 IP 电话接入，丰富的语音接入终端让用户使用高效、便捷。



小型分支运维部署

小型分支运维部署特点：

- 总部-分支场景部署

  总部根据整网规模，部署 eSight 企业版/专业版。

  分支设备的 snmp trap target-host 设置为总部网管地址。

  总部网管对全网设备（包括分支设备）自动发现并进行集中远程管理。也可通过 Telnet/SSH 对分支设备进行管理。

  总部安装部署 IPSec VPN、WLAN 等组件，实施增值业务管理。

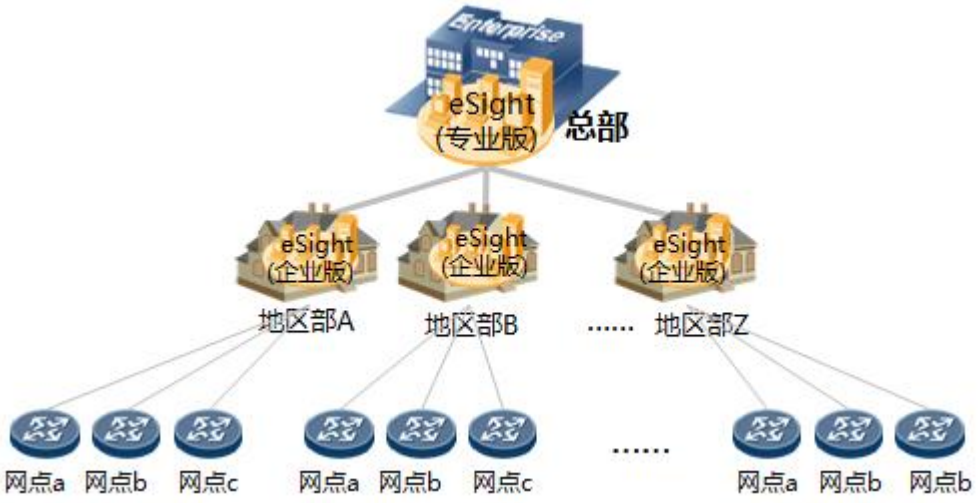
- 总部-分部-分支场景部署

  总部部署 eSight 专业版，分部部署 eSight 专业版，两者形成二级网管结构。

  分支设备的 snmp trap target-host 设置为总部网管地址。

  地区部网管对分部设备和下属分支设备自动发现并进行集中远程管理。也可通过 Telnet/SSH 对分支进行管理。

  总部安装部署 IPSec VPN、WLAN 等组件，实施增值业务管理。



4.2.4 典型配置建议（推荐产品、板卡）

小型分支产品推荐如下图：

规格/产品型号	AR200	AR1200	S2700
基础转发性能	450kpps	450kpps	1)8*FE+1*GeC 2)16*FE+2*GeC 3)24*FE+2*GEC 4)8*FE+1*FE 5)16*FE+2*FE 6)24*FE+2*FE 7)8*FE+1*GeC+POE 8)24*FE+2*GeC+POE
固定LAN口	8×FE电口	8×FE电口	
固定WAN口	AR201：1×电口FE AR206/7/8：1×xDSL AR207G：内置1×3G	2×GE电口	
支持插槽数	0	2个SIC槽（或1个WSIC）	
备注	1）AR200系列不支持插槽，通过子型号支持不同 2）207V支持8路语音，其它没有支持话音的型号 3）AR200无支持Wifi的款型 4）AR206/7/8区别在支持的xDSL类型不同	1）AR1220V支持IP语音 2）AR1220W支持Wifi 3）AR1220VW同时支持语音Wifi 4）支持插2块×3G SIC卡，形成3G主备链路上行	注： 1）S2700属于二层交换机。 2）S3700属于三层交换机。 3）Gec表示Ge Combo 4）POE表示下联口支持以太网供电

典型场景&产品选型如下图：

场景(小型分支)	需求	推荐产品	备注
小型金融网点(10～50信息点)	双E1上行；WLAN；语音	AR1220VW+2*E1 SIC卡+4FXS1FXO SIC卡（1块）。若语音口不够，则需选用AR2220。	1）AR200都不支持E1 2）AR200中除AR207G之外都不支持3G 3）AR200都不支持SIC卡 4）AR1220支持2SIC 5）常用SIC卡的类型： 4FXS＋1FXO 1 E1 2 E1 1 xDSL 2 xPON（GPON＋EPON） 1 HSPA＋7卡 1 GE Combo 1 cPOS WAN 6）常用WSIC卡的类型： 8FE＋1GE 2 CE1 2 FE WAN 语音单板除了4FXS+1FXO外，其它的没列
	双MSTP上行；WLAN；语音	AR1220VW+4FXS1FXO SIC卡（2块）	
	E1+xDSL上行；WLAN；语音	AR1220VW+E1 SIC卡+xDSL SIC卡（无法支持模拟语音，若要支持需选用AR2220）	
	E1+3G上行；WLAN；语音	AR1220VW+3G SIC卡/3G USB数据卡+E1 SIC卡。如果用3G USB卡，可用4FXS1FXO支持4路模拟语音，如果语音接入不够，建议用AR2220。	
小型企业分支	以太专线上行；WLAN；语音	AR1220VW+4FXS1FXO（2块）	
	xPON上行；WLAN；语音	AR1220VW+xPON SIC卡+4FXS1FXO（1块）。如果语音接口不够推荐AR2220+xPON SIC卡+语音卡	
小型政府机构/连锁超市	xDSL上行；WLAN	AR1220W+xDSL SIC卡	
	3G上行；WLAN	AR1220W+3G USB数据卡/3G SIC卡	
	E1/MSTP上行；WLAN	AR1220W+E1 SIC卡；AR1220W	

4.3 中型分支场景

4.3.1 对应的细分市场

中型分支网络主要针对于接入点 50 到 200 个场景，主要包括银行支行/小型分行,经济型酒店,中小医疗机构,中小企业等。

银行支行/小型分行

经济型酒店

中小医疗机构

中小企业

4.3.2 网络设计要点

中型分支网络设计要点：

- 两层网络设计

  核心层采用 AR2220/2240：配置 24GE 高密承担核心交换功能；配置 DSP 语音卡支持 VOIP，配置 FXS 卡支持模拟话机接入；采用固定扣或配置广域卡实现分支上行互联。接入交换机采用华为 S27/37 系列，交换机堆叠、上联链路捆绑。既提高可靠性，又简化管理。

- 安全设计

  AR 集成防火墙，支持安全域划分，可满足大多数场景需求。对安全要求苛刻场景，可旁挂或串联防火墙。旁挂防火墙，配置复杂；串联防火墙，网络层次多，可靠性不高。

- 分支语音

  AR2220 最多支持 128 路，AR2240 最多支持 384 路语音（IP 电话和模拟电话总和）。IP 电话连接二层交换机，模拟电话接 4/16/32FXS。

- 无线设计

  AP 连接 AR GE 口上行，AR 集成 AC 控制器，最多可管理 64AP+512 用户。

- 运维设计

  中型分支设备数量在 10 台以下，采用远程运维，本地不部署网管。

4.3.3 方案设计

针对中型分支网络的业务特点，华为融易分支中型分支网络的整体拓扑图如下。

设计方案总体特点：

- 两层网络设计：

  24GE 高密卡，满足核心交换和接入功能，免汇聚交换机部署，简化网络结构。

  接入交换机堆叠，上行链路捆绑，既简化管理，又提高可靠性。

  分支出口采用 WAN+Internet 方式

- 语音：

  AR 特有 32*FXS 卡，支持高密模拟话机接入，满足从模拟到 IP 的平滑演进。

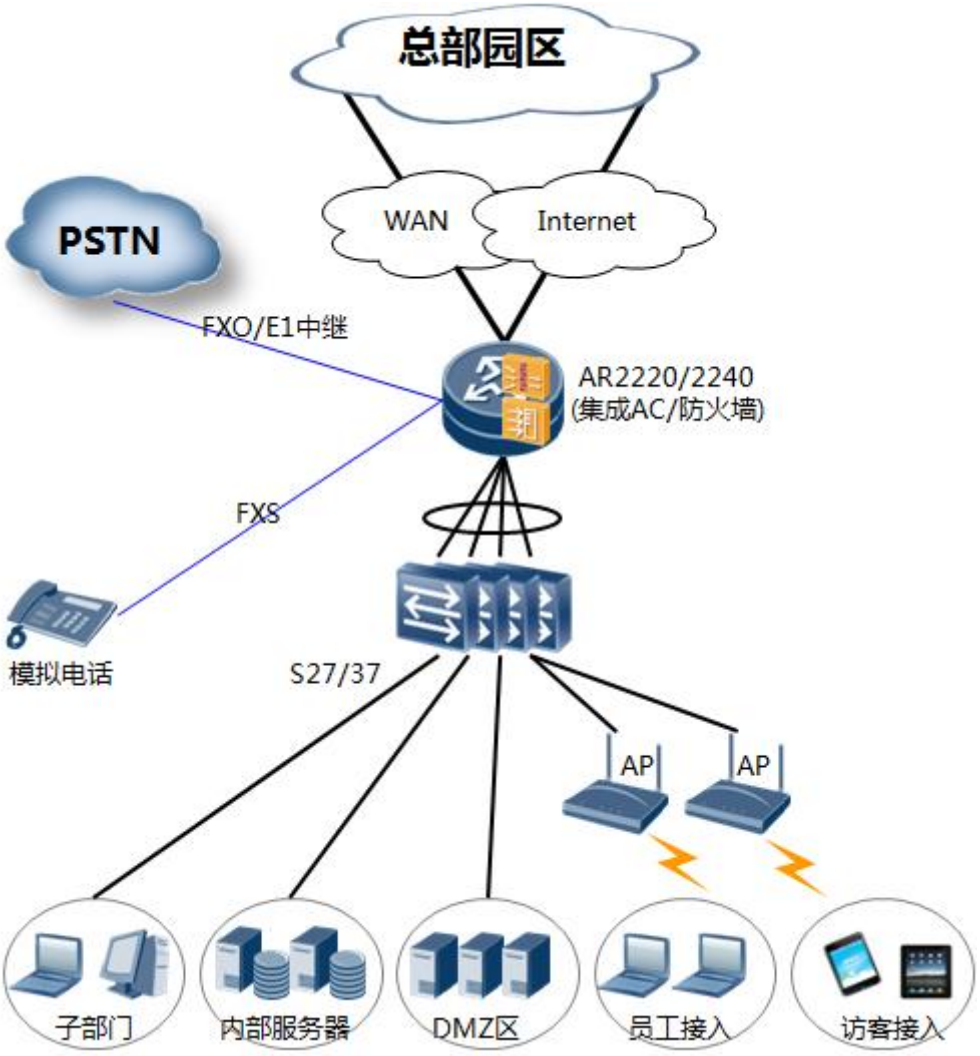
  AR 支持 IP PBX 模式、AG 模式，提供灵活的 VOIP 组网

- 安全：

  AR 集成防火墙，支持划分安全区域，满足大多数安全需求。IPSec 硬件加密隧道。

- 网管：

  总部部署网管，分支统一管理



中型分支无线部署

中型分支无线接入特点：

- 无线接入

  接入点采用华为 AP6xxx 系列设备，接入控制器采用 AR22xx 集成 AC 的方式。

  AP 连接带 POE 功能的交换机端口。

- 内部员工/访客隔离

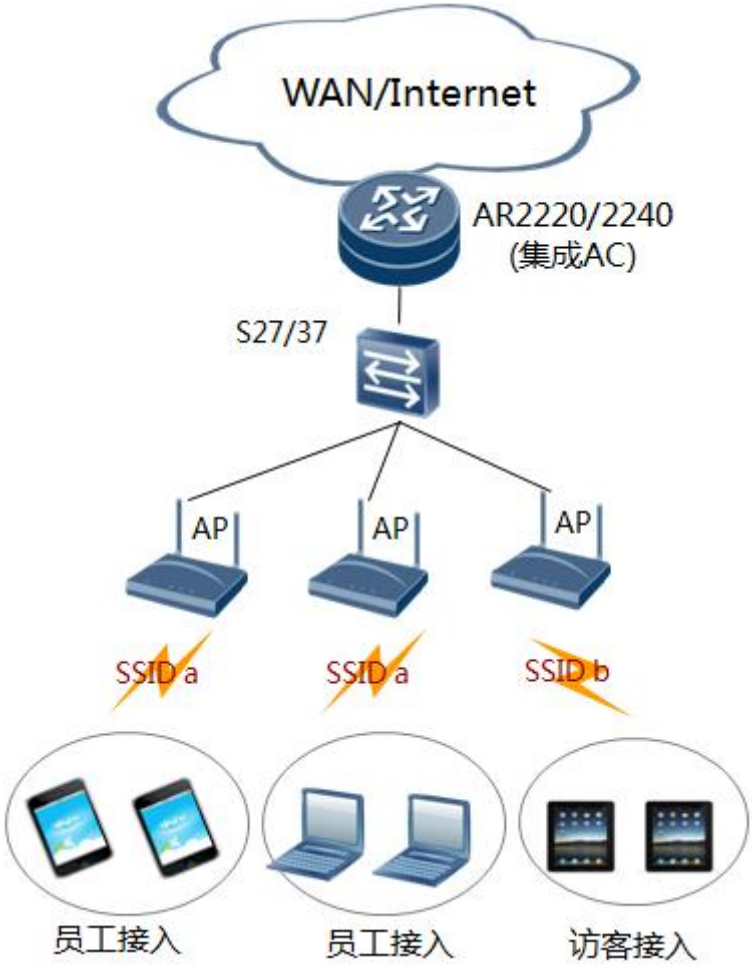
  AR 分别为内部员工和外部访客配置不同 SSID，分别对应不同子网，便于访问权限策略控制。

  开放内部员工访问内部网权限。开放访客子网到因特网权限。

- 安全认证

  对内部员工选择采用 802.1x 或 Portal 认证方式;对访客采用 Portal 认证方式。802.1x 安全性高，适合内部员工；Portal 认证不需安装客户端，适合访客。

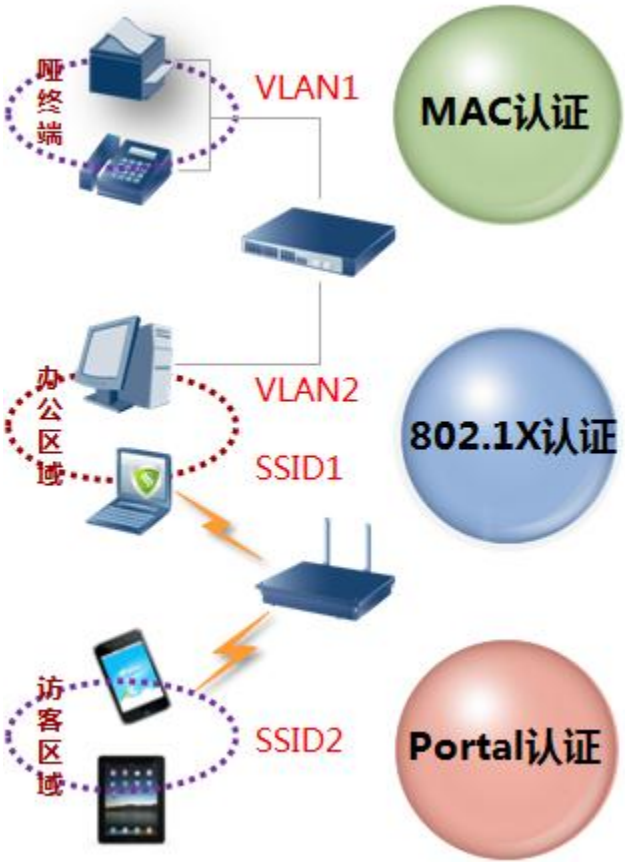
无线终端接入认证点位于集成的 AC，控制点位于 AP。认证/授权/计费等服务器、隔离域服务器、认证后域服务器在总部。



终端认证方式

终端认证方式的选择：

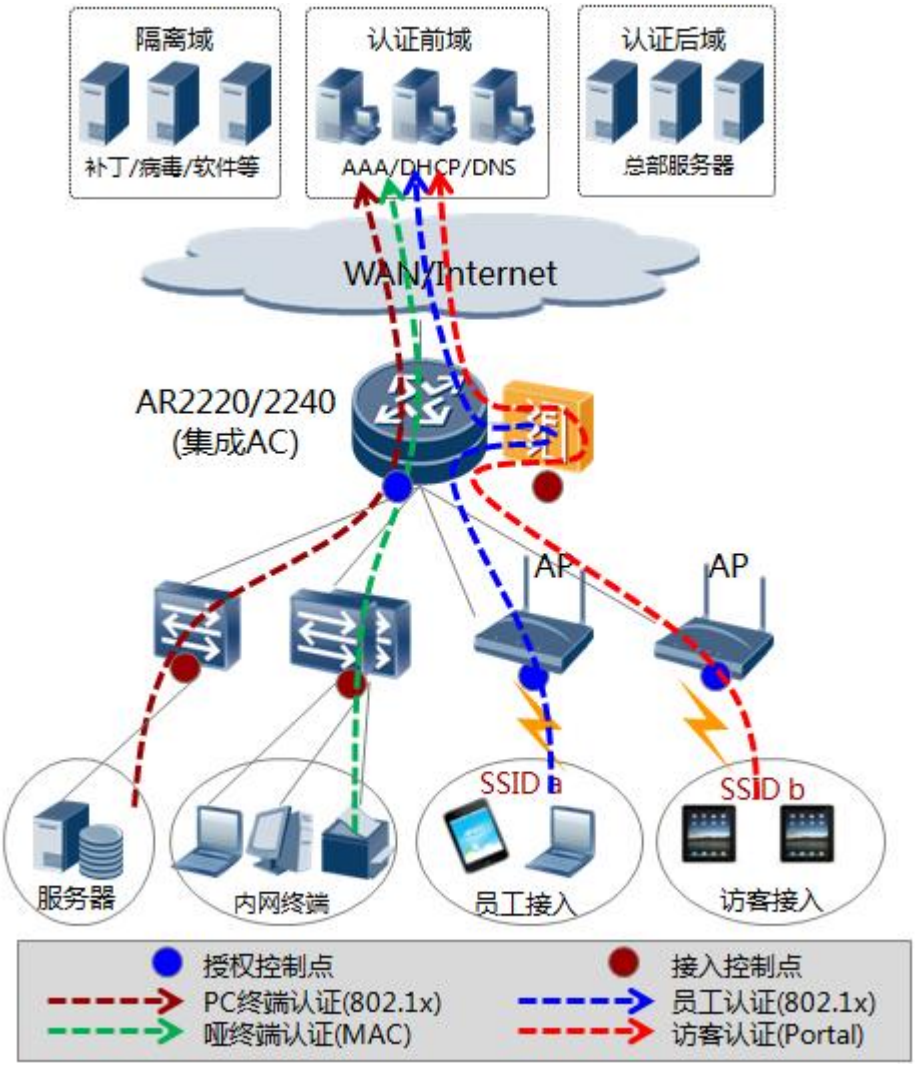
- 哑终端(包括 IP 电话机、打印机、传真机等)采用 MAC 认证
- 分支内部用户(有线接入)采用 802.1x 认证
- 分支内部用户(便携机、pad、智能手机无线接入) 采用 Portal 认证
- 访客终端(无线接入) 采用 Portal 认证



终端接入控制部署

终端接入控制部署的方式：

- 认证/授权服务器部署在总部
- 对有线用户：接入/授权控制点分别在接入交换机和 AR 路由器。AR 路由器启用 802.1X＋MAC 自适应认证，分别对应 PC 和哑终端。
- 对无线用户：接入点和控制点分别在 AC 和 AP。企业员工采用 802.1X 认证，访客采用 Portal 认证。



中型分支安全部署（内置防火墙）

中型分支安全部署（内置防火墙）特点：

- 安全域划分

  分支内网（包括各部门终端用户及服务器）、员工无线接入、WAN 出口、Internet 之上的 IPSec 隧道划归高优先级

  门户网站划归 DMZ 区，中优先级

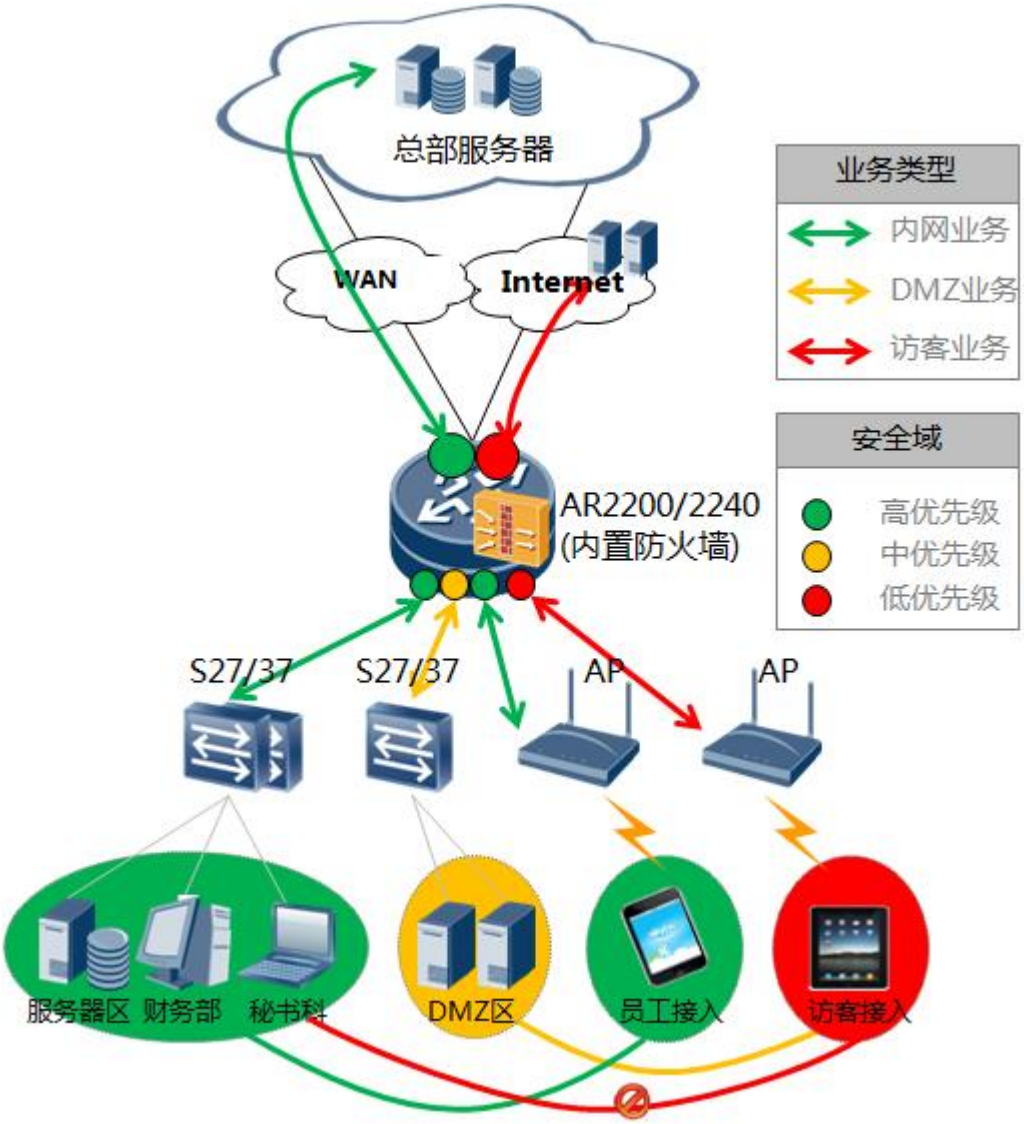
  访客和 Internet 出口划归低优先级

- 安全隔离(安全域)

  高优先级区域缺省可访问低优先级区域，低优先级区域访问高优先级区域需单独配置。

  分支内网三层隔离通过 ACL 实现。

  访客与 Internet 位于低优先级，缺省实现互访；同时开放位于 DMZ 区的门户网站。



中型分支安全部署（防火墙旁挂）

中型分支安全部署（内置防火墙）特点：

- 适用场景

  对于内部有门户网站的大/中型分支，对安全要求比较高，单纯采用 AR 集成防火墙无法阻止来自因特网的攻击，须采用专业防火墙做安全隔离。

- 方案设计

  出口路由器旁挂防火墙，工作在路由模式。

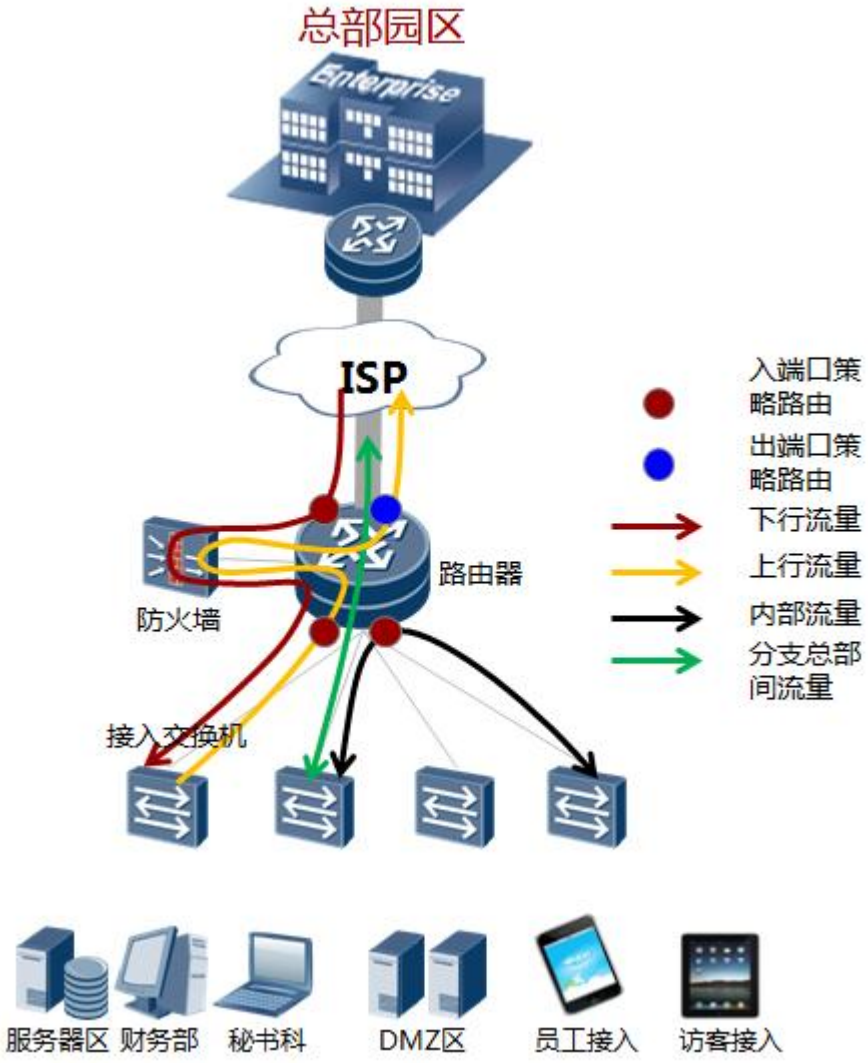
  路由器下联口的入方向配置策略路由：分支内部流量本地三层转发，不经防火墙；分支与总部间流量封装进 IPSec 隧道，不经防火墙；其它流量(上网流量)重定向到防火墙。

  路由器上联口的入方向配置所有流量重定向到防火墙。

- 方案优缺点

  优点：防火墙旁挂，出口路由器连接接入交换机，兼做汇聚交换，简化网络。

  缺点：需配置复杂的策略路由，运维困难



中型分支互联及因特网接入

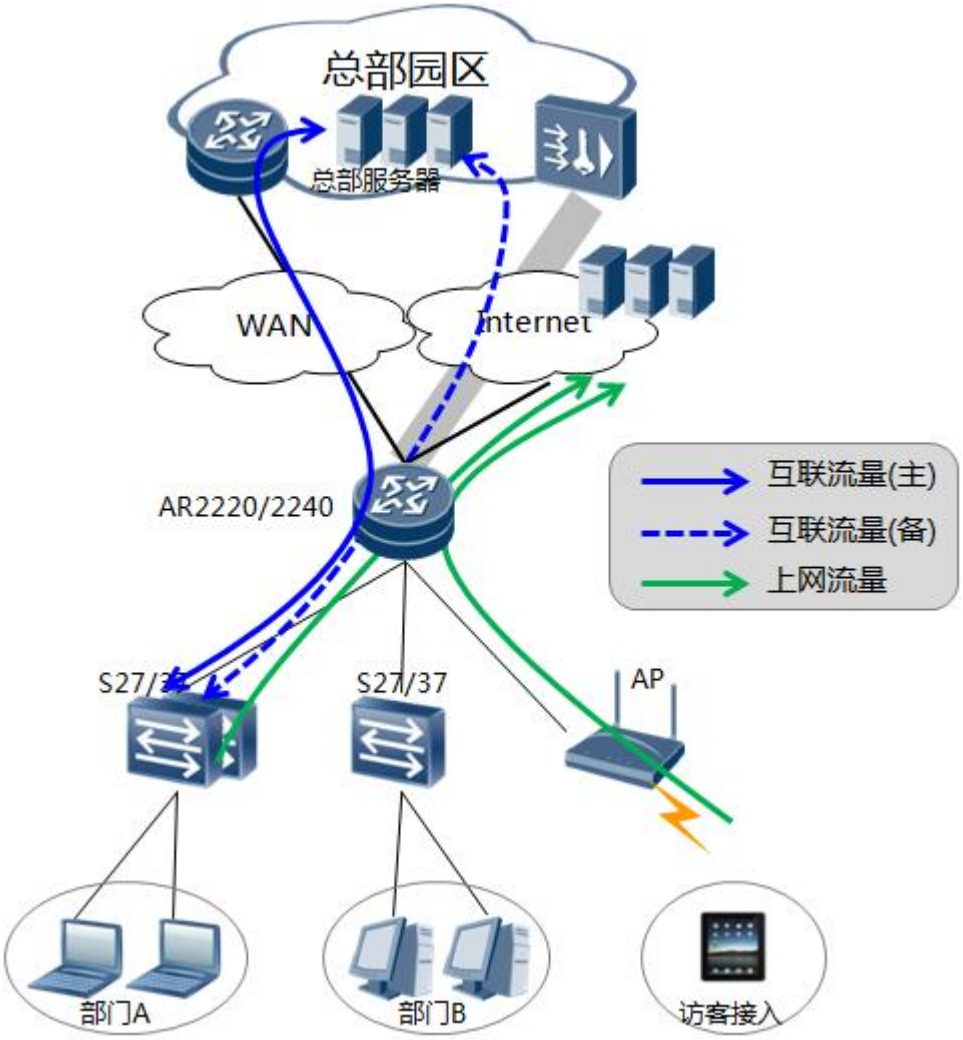
- 分支互联方式

  WAN 为互联主链路，用户根据各自情况选择链路类型和带宽；Internet 为备份链路，分支互联数据走 IPSec 隧道，中型分支推荐因特网专线(以太或 xPON 专线)。

- 因特网接入

  分支内部员工和访客通过 Internet 链路接入因特网，两类用户都为私网地址，出口路由器 AR 上做 NAT 影射。

  分支门户网站配置私网地址，固定 NAT 映射到公网 IP。



中型分支语音部署

中型分支语音部署特点：

- 适用场景

中型分支规模终端接入点在 50~200 左右，语音终端接入号码数小于 120。

典型场景如银行支行、中小医疗机构、经济型酒店等。

- 分支部署

  AR 配置语音功能，并部署 SIP-PBX 模式。

  SIP PBX 部署模式下，可以开始更多语音功能，如 IVR、CDR 功能。并可充分享受总部园区已有的语音补充业务，如电话会议功能。

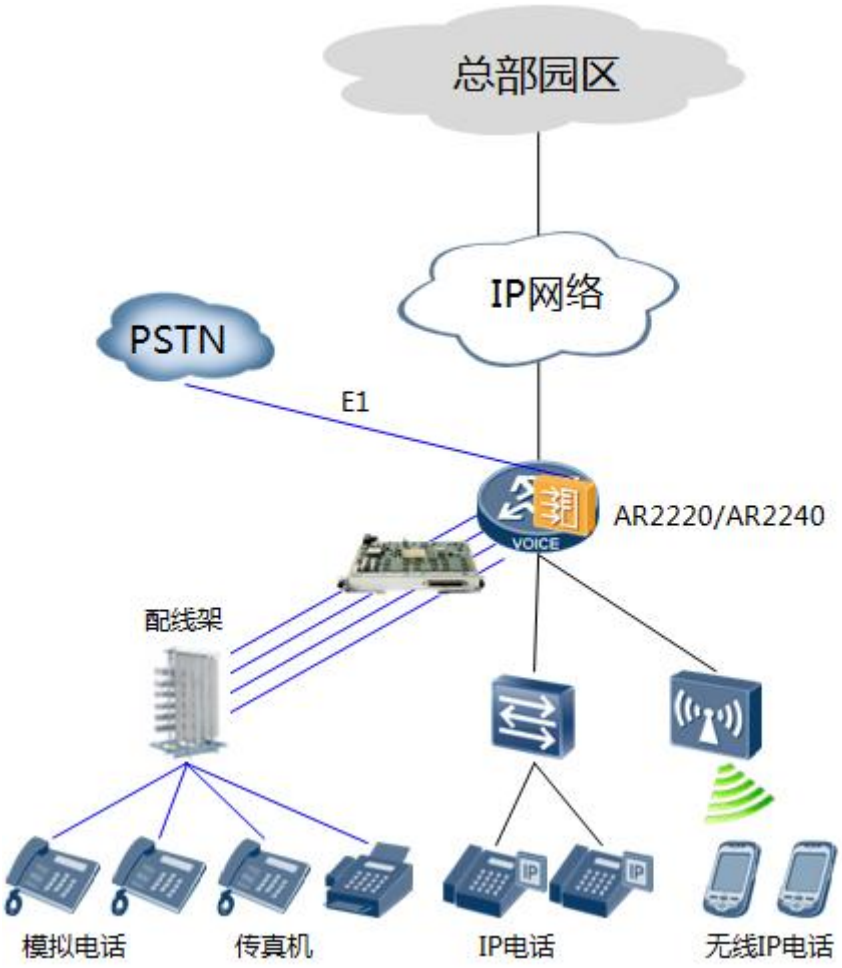
  AR 旁挂 AC+瘦 AP 提供无线 IP 电话的 WIFI 接入。

  AR 通过 E1 接入 PSTN，可同时多路跟外线互通。

- 客户价值

  支持模拟电话、有线、无线 IP 电话接入，丰富的语音接入终端让用户使用高效、便捷。

  AR2200/3200 支持 32FXS 高密语音板卡。最多可以支持 192 路模拟语音，大大满足语音接入数。



中型分支运维部署

中型分支运维部署特点：

- 总部-分支场景部署

  总部根据整网规模，部署 eSight 标准版/专业版。

  分支设备的 snmp trap target-host 设置为总部网管地址。

  总部网管对全网设备（包括分支设备）自动发现并进行集中远程管理。也可通过 Telnet/SSH 对分支设备进行管理。

  总部安装部署 IPSec VPN、WLAN 等组件，实施增值业务管理。