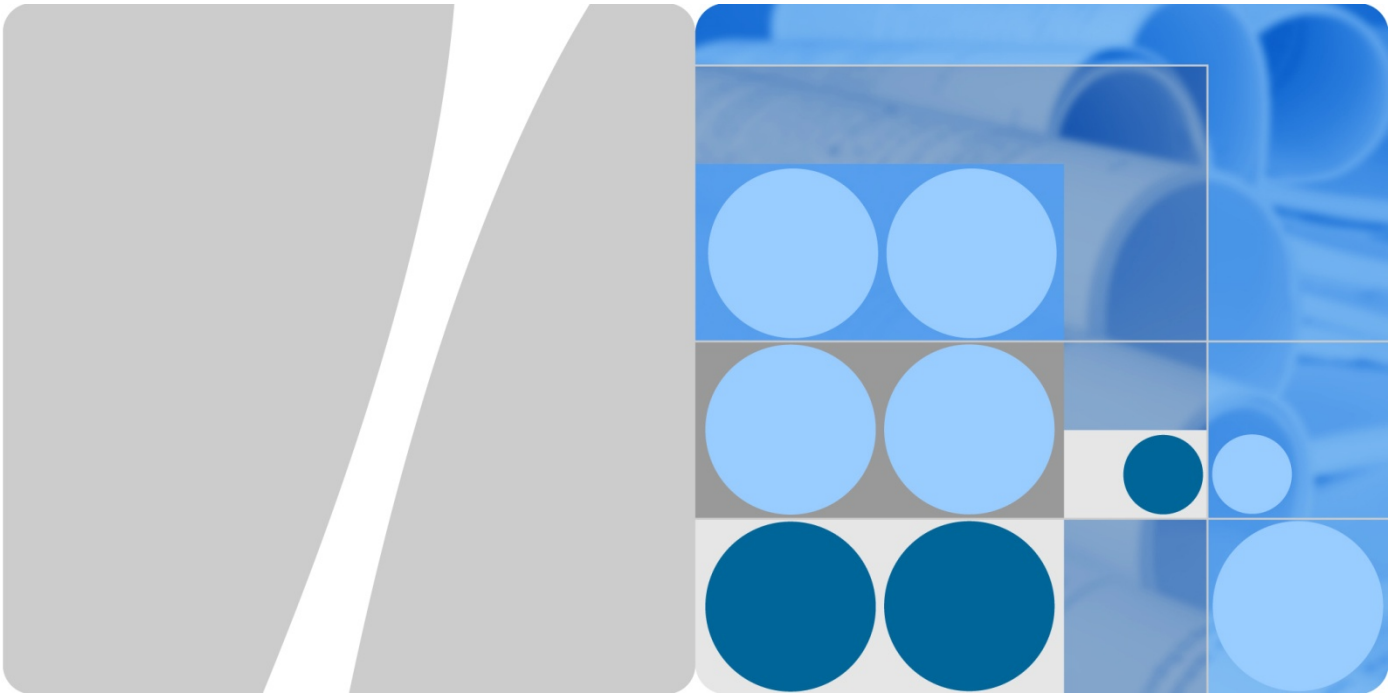


ONE NET Branch 中小企业网络解决方案

V100R001C00

技术建议书

文档版本 01

发布日期 2011-10-31

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

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

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

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 导言

1.1 中小企业解决方案概述

当前我国中小企业发展迅速，在国民经济和社会发展中的地位和作用与日增强，据统计中小企业占我国企业总数的 99%以上，创造的产品和价值占 GDP 的 60%，中小企业以其灵活的运行机制和市场适应能力成为推动中国经济社会发展的重要力量。

随着信息化时代的不断发展，中小企业追求更高效的沟通和交流管理方式，扩大自身的生产运营规模，增强企业的市场竞争力。这就要求以信息化为平台，以网络为承载媒介，提高企业的运作效率，降低运营成本，而网络建设无疑是其中最基本也是最重要的一个环节。华为公司从经济角度和企业规模角度将中小企业分为微型机构、小型机构、中小型机构和中型机构四种基础网络架构，中小企业可以根据自身的实际需要选择相应的网络建设方案。对于安全、无线接入、语音有特殊要求的中小企业，华为公司提供高级安全解决方案、高级无线解决方案和高级语音解决方案，并提供网络管理解决方案，满足不同层次中小企业的客户需求，保证网络建设质量的同时最大程度的节省企业的投资成本。

1.2 中小企业面临的困难

中小企业需要着重解决企业基础网络安全、业务部署灵活性和运维压力太大的问题，华为公司针对企业运维痛点提供的解决方案包含用户 NAC（Network Access Control）接入安全、园区边界安全、分支与远程接入、端到端语音部署、端到端无线部署、网络 TOPO 自动发现、服务器远程监控等方案，全面解决中小企业面临的基础网络安全和运维压力。

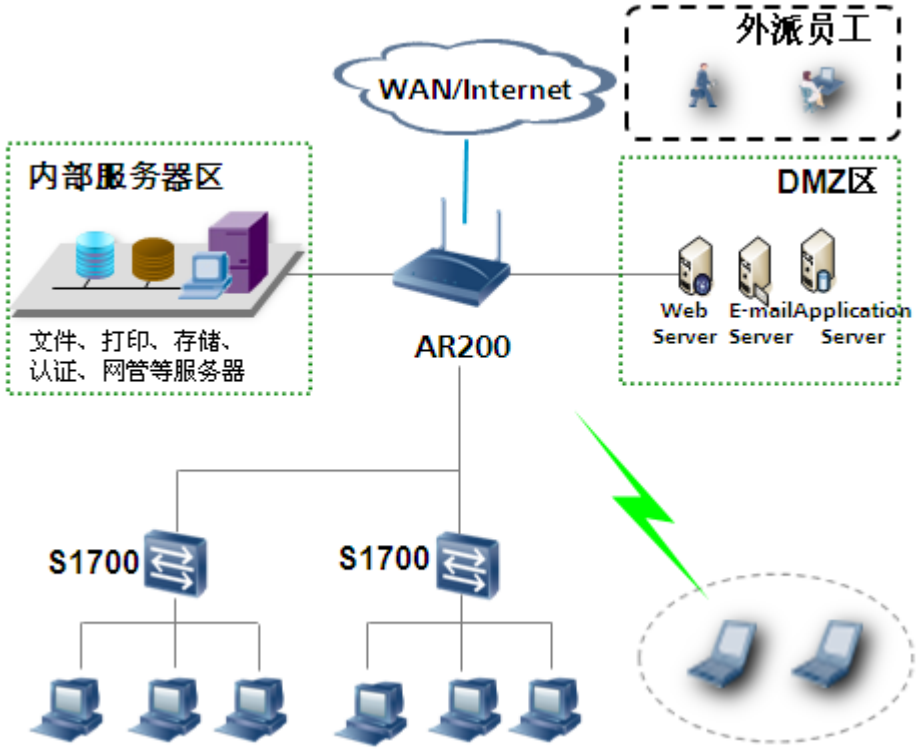
2 微型机构基础网络解决方案

2.1 微型机构基础网络设计原则

目前 50%以上的企业属于微型机构，典型的微型机构是小企业或大企业的分支办公室，这类机构通常为 0～50 信息点构成，因为企业员工数量少，业务需求单一，对企业网络有很高的经济性要求，对通信设备稳定度要求不高，只需要基础网络能够支撑工作基本需要的 Email、打印、终端互联即可。

微型机构基础网络场景以低端 AR 路由器为中心搭建公司网络，AR 承担作为企业网关，并支持 Web、打印、认证、Email 等业务接入，无线终端和有线终端的混合接入，同时 AR 路由器集成简单防火墙功能，提供边界安全。企业可以通过增加低成本交换机扩展接入范围，以提升扩展性。

图2-1 微型机构基础网络物理架构



2.2 微型机构基础网络规划

2.2.1 核心层设计规划

核心层用于转发各部门之间的流量。考虑到企业初期建设成本，采用 AR200 路由器作为核心层设备，与微型企业内部服务器区、DMZ（Demilitarized Zone）区、Internet 区和内部业务区进行互联，支撑企业内外部的业务流量。

2.2.2 接入层设计规划

接入层是最靠近用户的网络，为用户提供各种接入方式，是终端、边缘和 IP 电话等设备接入网络的第一层。一般都部署二层设备，有线用户通过 S1700 接入 AR200，无线用户通过 AR200 自带的 WLAN 功能进行无线接入。

2.2.3 出口设计规划

微型机构通过 AR 获取公网地址，实现与 WAN/Internet 的互访，可以采用设置 IP 静态地址或 PPP（Point-to-Point Protocol）动态方式获取公网地址。

2.2.4 安全性设计规划

通过 AR200 集成防火墙功能解决如下安全问题：

- 微型机构内、外网之间的访问控制，实现微型机构内、外网的安全隔离。
- 外派员工与微型机构 DMZ 区的访问控制，实现外派员工与内网的安全隔离。

2.3 微型机构基础网络业务方案

2.3.1 数据业务规划

- 有线用户数据业务：

  S1700 交换机作为二层接入设备，通过 VLAN 划分用户。AR 路由器作为三层网关，通过 DHCP（Dynamic Host Configuration Protocol）方式为有线用户分配 IP 地址。企业可以根据自身分区情况，划分多个 IP 地址段。AR 上行通过公网地址接入 WAN/Internet 网络，通过 AR 做 NAT，进行私网地址到公网地址的转换，实现有线用户与 WAN/Internet 网络的互访。

- 无线用户数据业务：

  AR 作为胖 AP，无线用户通过 PSK 方式接入 AR，AR 路由器作为三层网关，通过 DHCP 方式为无线用户分配 IP 地址。AR 上行通过公网地址接入 WAN/Internet 网络，通过 AR 做 NAT，进行私网地址到公网地址的转换，实现无线用户与 WAN/Internet 网络的互访。

- 外派员工数据业务：

  外派员工通过 IPSec VPN 方式与微型机构建立隧道，实现外派员工与微型机构的互访。可以在外派员工的电脑中安装硬件或通过纯软件方式来实现 IPSec VPN 功能。

- 服务器数据业务：

  企业事先规划好服务器区和 DMZ 的服务器地址，服务器使用静态地址，内部服务器区和 DMZ 区的服务器以 AR 作为网关。

2.3.2 语音业务规划

考虑到微型机构人数有限，同城微型机构建议 AR 作为 AG 场景应用，用户语音信息到总部注册，由总部统一分配号码及管理。异地微型机构建议 AR 作为 PBX（Private Branch Exchange）场景应用，用户语音信息到 PBX 注册，接入当地 PSTN（Public Switched Telephone Network）网络，具体内容请参见 8 中小型机构高级语音解决方案。

2.3.3 安全业务规划

微型机构通常人数有限，不建议对用户接入进行权限控制，如企业有特殊需求，可以采用华为公司 NAC 方案，具体内容请参见 6 中小型机构高级安全解决方案。

2.4 微型机构基础网络技术方案

2.4.1 VLAN 设计

VLAN 是将 LAN 内的设备逻辑地而不是物理地划分为一个个网段，从而实现在一个 LAN 内隔离广播域的技术。既隔离了广播域，减少了广播风暴，又增强了信息的安全性。

- VLAN 通常根据业务需要进行规划，需要隔离的端口配置不同的 VLAN，需要防止广播域过大的地方配置 VLAN 用于减小广播域。
- VLAN 最好不要跨交换机，即使跨交换机，数目也需要限制。
- S1700 根据接入位置为不同 PC 分配不同的 VLAN，不同 S1700 交换机采用不同的 VLAN，避免广播域过大，利于问题及时定位。

2.4.2 IP 设计

- IP 地址分为动态 IP 与静态 IP 的选取，原则上服务器、特殊终端设备建议采用静态 IP。办公用设备建议使用 DHCP 动态获取（如办公用 PC 等）。
- AR200 上行优选固定 IP 地址接入，其次选择 PPP 方式接入。AR 作为 DHCP 网关和 DHCP Server，为有线、无线用户分配私网 IP 地址。
- 服务器采用静态 IP 地址接入。

2.4.3 DHCP 设计

DHCP 部署的基本原则为固定 IP 地址段和动态分配 IP 地址段保持连续，按照业务区域进行 DHCP 地址的划分，便于统一管理及问题定位。启动 DHCP 安全功能，禁止非法 DHCP Server 的架设和非法用户的接入。

AR 作为 DHCP 网关和 DHCP Server，为有线、无线用户分配私网 IP 地址。有线用户通过 S1700 交换机携带 VLAN 信息，AR 终结 VLAN 并给有线用户分配私网 IP 地址。无线用户通过 PSK 方式接入 AR，AR 终结无线报文，作为无线用户网关分配私网 IP 地址。

2.4.4 NAT 设计

NAT（Network Address Translation）用于实现私有网络和公有网络之间的互访。微型机构内部使用私有 IP 地址，微型机构出口 AR 使用公网地址与外界通信，AR 需要部署 NAT 特性，实现用户侧私网地址到网络侧公网地址的转换，实现用户与 WAN/Internet 的互访。

2.4.5 安全设计

AR 部署防火墙功能，将 WAN/Internet 区域划分为 untrust 区域，公用服务器区域划分为 DMZ 区，其他区域划分为 trust 区域。允许 trust 区域和 DMZ 区域互访，允许 untrust 区域与 DMZ 区域互访，不允许 trust 区域和 untrust 区域之间的直接互访。

基于安全考虑，建议 AR 部署 ARP（Address Resolution Protocol）防攻击功能，以防止非法的 ARP 报文对网络的攻击。

2.4.6 远程接入设计

微型机构访问 WAN/Internet 通过 AR 的 NAT 功能实现。

外派员工通过 IPSec VPN 访问微型机构。建议采用 ESP 封装模式，封装新的 IP 报文头并对原始数据报文进行加密，更为安全。

2.4.7 网管设计

AR 和 S1700 交换机通过 Web 网管进行配置管理及日常网络维护。

2.5 微型机构基础网络方案特点

- 高性价比：低投资、高性能、经济的网络。
- 简易性：结构清晰、简单、安装便捷，无需配置专职维护人员。
- 绿色环保：全方位节能设计、无风扇、省电无噪声。

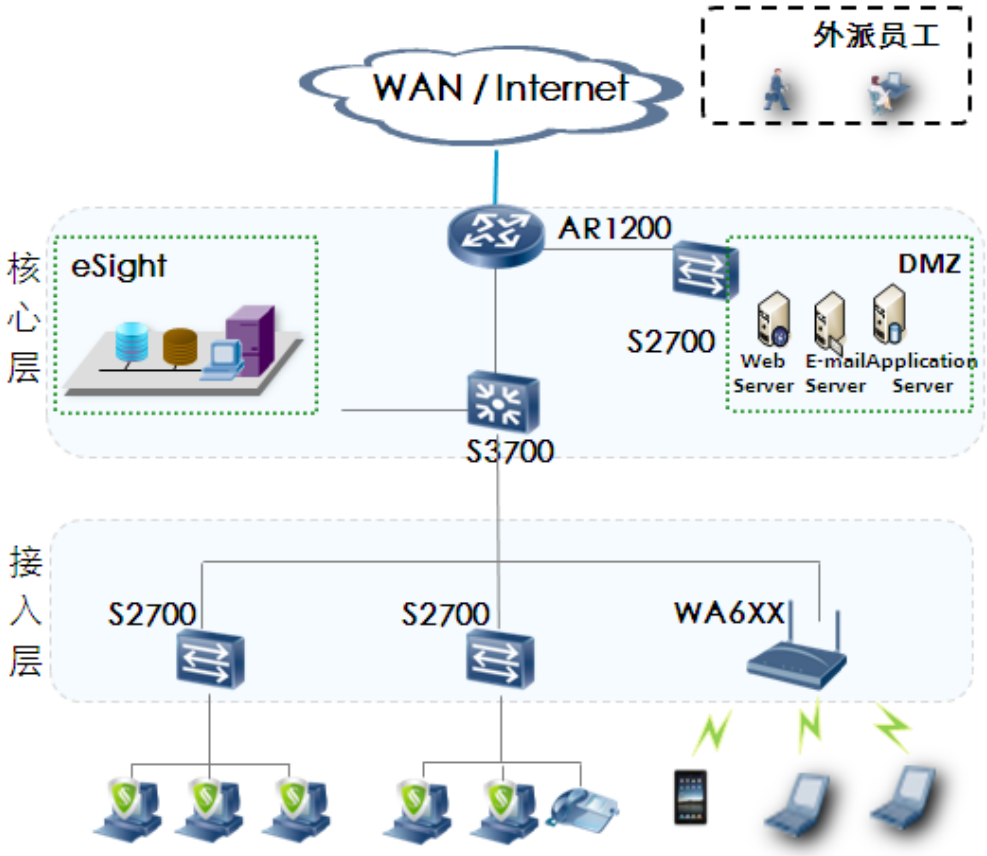
3 小型机构基础网络解决方案

3.1 小型机构基础网络设计原则

典型的小型机构是小企业或大企业的分支办公室，这类机构通常由50～100信息点构成，因为企业已经达到一定规模，较大的业务量和员工数量都要求网络具备更高的稳定性，可扩展性，安全性，同时毕竟企业规模没有达到更大的规模，仍然需要网络经济、简洁便于维护。

小型机构基础网络场景的方案特点以中低端交换机为中心搭建公司网络交换平台，该交换机作为中心汇聚点，通过其他低端交换机实现业务和终端的接入，并通过 AR 作为企业出口路由器，实现 WAN 和 Internet 互联，AR 路由器集成简单防火墙功能，提供边界安全。

图3-1 小型机构基础网络物理架构



3.2 小型机构基础网络规划

3.2.1 核心层设计规划

核心层用于转发各部门之间的流量，采用 AR1200 路由器作为核心层出口设备，S3700 系列交换机汇聚内部服务器区和接入区流量，使内部服务器区、DMZ 区、Internet 区和内部业务区进行互联，支撑内外部的业务流量。

3.2.2 接入层设计规划

接入层是最靠近用户的网络，为用户提供各种接入方式，是终端、边缘和 IP 电话等设备接入网络的第一层，一般都部署二层设备。

有线用户通过 S2700 交换机接入、S3700 交换机汇聚流量到 AR1200 进行有线接入，无线用户通过 WA600 系列胖 AP 进行无线接入。

3.2.3 出口设计规划

小型机构通过 AR 获取公网地址，实现与 WAN/Internet 的互访，可以采用设置 IP 静态地址或 PPP 动态方式获取公网地址。

3.2.4 安全性设计规划

通过 AR1200 集成防火墙功能解决如下安全问题：

- 小型机构内、外网之间的访问控制，实现小型机构内、外网的安全隔离。
- 外派员工与小型机构 DMZ 区的访问控制，实现外派员工与内网的安全隔离。

3.3 小型机构基础网络业务方案

3.3.1 数据业务规划

- 有线用户数据业务：

  S2700 交换机作为二层接入设备，通过 VLAN 划分用户。S3700 交换机作为汇聚交换机聚合各接入交换机上送的 VLAN 流量到 AR1200，AR1200 通过 DHCP 方式为有线用户分配 IP 地址。企业可以根据自身分区情况，划分多个 IP 地址段。AR1200 上行通过公网地址接入 WAN/Internet 网络，通过 AR 做 NAT，进行私网地址到公网地址的转换，实现有线用户与 WAN/Internet 网络的互访。

- 无线用户数据业务：

  WA600 系列 AP 作为胖 AP，无线用户通过 PSK 方式接入 WA600 系列 AP，AR1200 作为三层网关，通过 DHCP 方式为无线用户分配 IP 地址。AR1200 上行通过公网地址接入 WAN/Internet 网络，通过 AR1200 做 NAT，进行私网地址到公网地址的转换，实现无线用户与 WAN/Internet 网络的互访。

- 外派员工数据业务：

  外派员工通过 IPSec VPN 方式与小型机构建立隧道，实现外派员工与小型机构的互访。可以在外派员工的电脑中安装硬件或通过纯软件方式来实现 IPSec VPN 功能。

- 服务器数据业务：

  企业事先规划好服务器区和 DMZ 的服务器地址，服务器使用静态地址，S2700 交换机作为二层接入设备，通过 VLAN 划分服务器，内部服务器区和 DMZ 区的服务器以 AR1200 作为网关。

3.3.2 语音业务规划

基于小型机构人数规模，如果总部需要对小型机构进行控制，则 AR 作为 AG 场景应用，用户语音信息到总部注册，由总部统一分配号码及管理，可以由总部提供丰富的语音业务，但是会增加总部的负荷。如果小型机构需要自行进行控制，则 AR 作为 PBX 场景应用，用户语音信息到 AR 注册，由 AR 统一分配号码及管理，减轻了总部的负荷，但是无法使用总部提供的丰富的语音业务。具体内容请参见 8 中小型机构高级语音解决方案。

3.3.3 安全业务规划

如果需要对用户的接入安全进行控制，则建议部署 NAC 方案。可以采用在 S2700 交换机上部署 802.1X 认证或者在 AR 上部署 Portal 认证的方式，均可以实现对用户接入的安全控制，具体内容请参见 6 中小型机构高级安全解决方案。

3.4 小型机构基础网络技术方案

3.4.1 VLAN 设计

VLAN 是将 LAN 内的设备逻辑地而不是物理地划分为一个个网段，从而实现在一个 LAN 内隔离广播域的技术。VLAN 技术既隔离了广播域，减少了广播风暴，又增强了信息的安全性。

- VLAN 通常根据业务需要进行规划，需要隔离的端口配置不同的 VLAN，需要防止广播域过大的地方配置 VLAN 用于减小广播域。
- VLAN 最好不要跨交换机，即使跨交换机，数目也需要限制。
- S2700 根据接入位置为不同 PC 分配不同的 VLAN，不同 S2700 交换机采用不同的 VLAN，避免广播域过大，利于问题及时定位。
- S3700 交换机汇聚 S2700 交换机的 VLAN 信息，透传给 AR1200 设备，实现 VLAN 的终结。

3.4.2 IP 设计

IP 地址分为动态 IP 与静态 IP 的选取，原则上服务器、特殊终端设备建议采用静态 IP。办公用设备建议使用 DHCP 动态获取如办公用 PC 等。

AR1200 上行优选固定 IP 地址接入，其次选择 PPP 方式接入。AR1200 作为 DHCP 网关和 DHCP Server，为有线、无线用户分配私网 IP 地址。服务器采用静态 IP 地址接入。

3.4.3 DHCP 设计

DHCP 部署基本原则为固定 IP 地址段和动态分配 IP 地址段保持连续，按照业务区域进行 DHCP 地址的划分，便于统一管理及问题定位。启动 DHCP 安全功能，禁止非法 DHCP Server 的架设和非法用户的接入。

AR1200 作为 DHCP 网关和 DHCP Server，为有线、无线用户分配私网 IP 地址。

- 有线用户通过 S2700 交换机携带 VLAN 信息，S3700 交换机聚合 S2700 交换机上送的 VLAN 流量到 AR1200，AR1200 终结 VLAN 后给有线用户分配私网 IP 地址。
- 无线用户通过 PSK 方式接入 WA600 系列 AP，WA600 系列 AP 终结无线报文，二层透传无线用户的 DHCP 请求报文，AR1200 终结 VLAN 后给无线用户分配私网 IP 地址。

3.4.4 NAT 设计

NAT 称为网络地址转换，用于实现私有网络和公有网络之间的互访。小型机构内部使用私有 IP 地址，小型机构出口 AR 使用公网地址与外界通信，AR 需要部署 NAT 特性，实现用户侧私网地址到网络侧公网地址的转换，实现用户与 WAN/Internet 的互访。

3.4.5 安全设计

AR 部署防火墙功能，将 WAN/Internet 区域划分为 untrust 区域，公用服务器区域划分为 DMZ 区，其他区域划分为 trust 区域。允许 trust 区域和 DMZ 区域互访，允许 untrust 区域与 DMZ 区域互访，不允许 trust 区域和 untrust 区域之间直接互访。

基于安全考虑，建议 AR 部署 ARP 防攻击功能，接入交换机部署 DHCP Snooping 功能，以防止非法的 ARP 报文对网络的攻击。

3.4.6 远程接入设计

小型机构访问 WAN/Internet 通过 AR 的 NAT 功能实现。外派员工通过 IPSec VPN 访问小型机构。建议采用 ESP 封装模式，封装新的 IP 报文头并对原始数据报文进行加密，更为安全。

3.4.7 网管设计

部署 eSight 网管系统进行日常网络维护。

3.5 小型机构基础网络方案特点

- 可扩展：低投资、高性能，灵活网络架构易扩展，保护已有投资。
- 易维护：扁平网络，层次少，简易网管配置简单，无需专职网管人员。
- 区域划分清晰：部门间物理/逻辑隔离，保证业务安全，易排错。
- 绿色节能：绿色节能、无噪音。

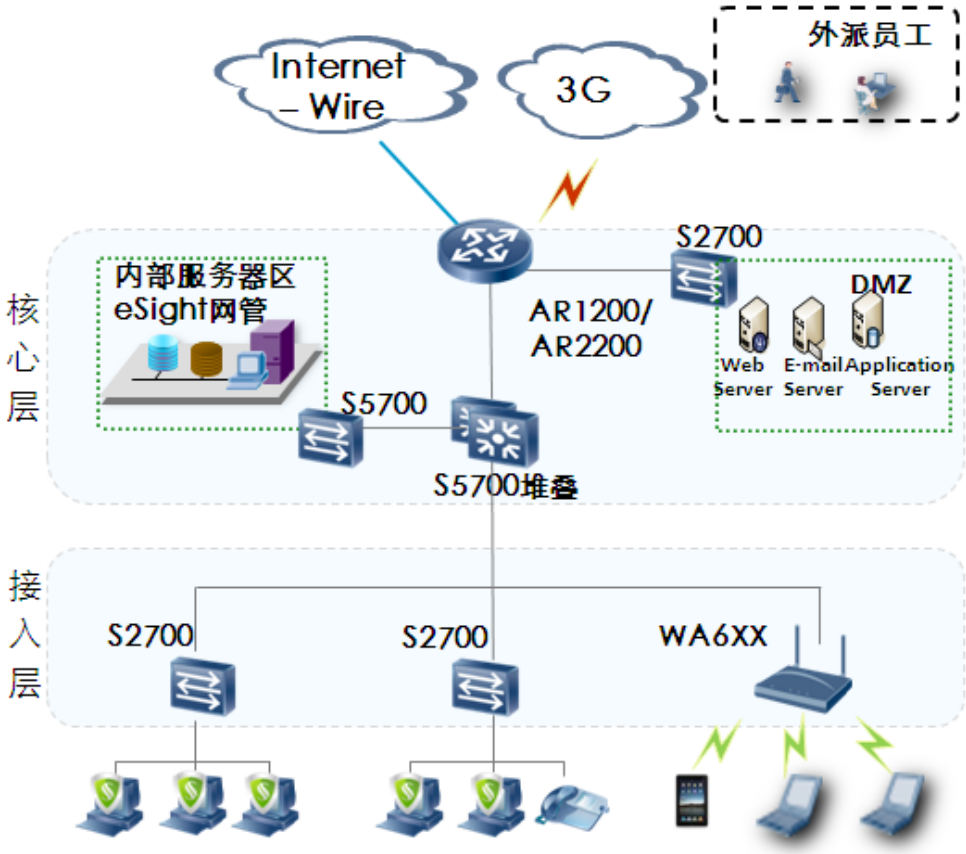
4 中小型机构基础网络解决方案

4.1 中小型机构基础网络设计原则

中小型机构通常为 100～300 信息点。中小型机构基础网络场景的方案特点是期待语音、数据、安全、移动业务丰富，希望获得一体化方案、一站式服务。

中小型企业的组网结构和小型企业类似，但因为企业规模的进一步扩大，有更强的企业内部互联以及企业出口的要求，对网络可靠性、可扩展性、安全性有一定的要求。这些要求体现在设备上，就是需要功能更强的 AR 作为企业出口路由器、需要通过链路备份机制提高可靠性、通过中心交换机的双备份以及流量分担。

图4-1 中小型机构基础网络物理架构



4.2 中小型机构基础网络规划

4.2.1 核心层设计规划

核心层用于转发各部门之间的流量，采用 AR1200/AR2200 路由器作为核心层出口设备，S5700 系列交换机汇聚内部服务器区、DMZ 区和接入区流量，使内部服务器区、DMZ 区、Internet 区和内部业务区进行互联，支撑内外部的业务流量。

4.2.2 接入层设计规划

接入层是最靠近用户的网络，为用户提供各种接入方式，是终端、边缘和 IP 电话等设备接入网络的第一层，一般都部署二层设备。

- 有线用户通过 S2700 交换机接入，S5700 交换机汇聚 S2700 交换机上送的 VLAN 流量到 AR1200/AR2200 进行有线接入。
- 无线用户通过 WA600 系列胖 AP 进行无线接入。

4.2.3 出口设计规划

中小型机构通过 AR 获取公网地址，实现与 WAN/Internet 的互访，可以采用设置 IP 静态地址或 PPP 动态方式获取公网地址。

4.2.4 可靠性设计规划

AR 上行采用 WAN 和 3G 链路备份方式，以 WAN 侧链路为主用链路，3G 链路平时不使用，仅作为备份。S5700 交换机采用堆叠技术，将多台 S5700 交换机虚拟化为 1 台设备，一旦主用 S5700 交换机出现故障后，其他交换机能立即接替其成为主用交换机。

4.2.5 安全性设计规划

通过 AR1200/AR2200 集成防火墙功能解决如下安全问题：

- 中小型机构内、外网之间的访问控制，实现中小型机构内、外网的安全隔离。
- 外派员工与中小型机构 DMZ 区的访问控制，实现外派员工与内网的安全隔离。

4.3 中小型机构基础网络业务方案

4.3.1 数据业务规划

- 有线用户数据业务：

  S2700 交换机作为二层接入设备，通过 VLAN 划分用户。S5700 交换机作为汇聚交换机聚合各接入交换机的 VLAN 流量，AR1200/AR2200 通过 DHCP 方式为有线用户分配 IP 地址。企业可以根据自身分区情况，划分多个 IP 地址段。AR1200/AR2200 上行通过公网地址接入 WAN/Internet、3G 网络，通过 AR1200/AR2200 做 NAT，进行私网地址到公网地址的转换，实现有线用户与 WAN/Internet 网络的互访。

- 无线用户数据业务：

  WA600 系列 AP 作为胖 AP，无线用户通过 PSK 方式接入 WA600 系列 AP，AR1200/AR2200 作为三层网关，通过 DHCP 方式为无线用户分配 IP 地址。AR1200/AR2200 上行通过公网地址接入 WAN/Internet 网络，通过 AR1200/AR2200 做 NAT，进行私网地址到公网地址的转换，实现无线用户与 WAN/Internet 网络的互访。

- 外派员工数据业务：

  外派员工通过 IPSec VPN 方式与中小型机构建立隧道，实现外派员工与中小型机构的互访。可以在外派员工的电脑中安装硬件或通过纯软件方式来实现 IPSec VPN 功能。

- 服务器数据业务：

  企业事先规划好服务器区和 DMZ 的服务器地址，服务器使用静态地址。S2700 交换机作为二层接入设备，通过 VLAN 划分服务器，内部服务器区和 DMZ 区的服务器以 AR1200/AR2200 作为网关。

4.3.2 语音业务规划

基于中小型机构人数规模，如果总部需要对中小型机构进行控制，则 AR 作为 AG 场景应用，用户语音信息到总部注册，由总部统一分配号码及管理，可以由总部提供丰富的语音业务，但是会增加总部的负荷。如果中小型需要自行进行控制，则 AR 作为 PBX 场景应用，用户语音信息到 AR 注册，由 AR 统一分配号码及管理，减轻了总部的负荷，但是无法使用总部提供的丰富的语音业务。具体内容请参见 8 中小型机构高级语音解决方案。

4.3.3 安全业务规划

如果需要对用户的接入安全进行控制，则建议部署 NAC 方案。可以采用在 S27 系列交换机上部署 802.1X 认证或者在 AR 上部署 Portal 认证的方式，均可以实现对用户接入的安全控制，具体内容请参见 6 中小型机构高级安全解决方案。

4.4 中小型机构基础网络技术方案

4.4.1 VLAN 设计

VLAN 是将 LAN 内的设备逻辑地而不是物理地划分为一个个网段，从而实现在一个 LAN 内隔离广播域的技术。VLAN 技术既隔离了广播域，减少了广播风暴，又增强了信息的安全性。

- VLAN 通常根据业务需要进行规划，需要隔离的端口配置不同的 VLAN，需要防止广播域过大的地方配置 VLAN 用于减小广播域。
- VLAN 最好不要跨交换机，即使跨交换机数目也需要限制。
- S2700 根据接入位置为不同 PC 分配不同的 VLAN，不同 S2700 交换机采用不同的 VLAN，避免广播域过大，利于问题及时定位。
- S5700 交换机汇聚 S2700 交换机的 VLAN 信息，透传给 AR1200/AR2200 设备，实现 VLAN 的终结。

4.4.2 IP 设计

IP 地址分为动态 IP 与静态 IP 的选取，原则上服务器、特殊终端设备建议采用静态 IP。办公用设备建议使用 DHCP 动态获取（如办公用 PC 等）。

AR1200/AR2200 上行优选固定 IP 地址接入，其次选择 PPP 方式接入。AR1200/AR2200 作为 DHCP 网关和 DHCP Server，为有线、无线用户分配私网 IP 地址。服务器采用静态 IP 地址接入。

4.4.3 DHCP 设计

DHCP 部署基本原则为固定 IP 地址段和动态分配 IP 地址段保持连续，按照业务区域进行 DHCP 地址的划分，便于统一管理及问题定位。启动 DHCP 安全功能，禁止非法 DHCP Server 的架设和非法用户的接入。

AR1200/AR2200 作为 DHCP 网关和 DHCP Server，为有线、无线用户分配私网 IP 地址。

- 有线用户通过S2700交换机携带VLAN信息，S5700交换机汇聚S2700上送的VLAN流量 AR1200/AR2200，AR1200/AR2200 终结 VLAN 并给有线用户分配私网 IP 地址。
- 无线用户通过 PSK 方式接入 WA600 系列 AP，WA600 系列 AP 终结无线报文，二层透传无线用户的 DHCP 请求报文，AR1200/AR2200 终结 VLAN 后给无线用户分配私网 IP 地址。

4.4.4 NAT 设计

NAT 称为网络地址转换，用于实现私有网络和公有网络之间的互访。AR 部署 NAT 特性，实现用户侧私网地址到网络侧公网地址的转换，实现用户与 WAN/Internet 的互访。在中小型机构基础网络场景中，WAN 侧和 3G 侧都需要部署 NAT 特性，以防止某侧链路出现故障后仍能实现私网地址到公网地址的转换。

4.4.5 安全设计

AR 部署防火墙功能，将 WAN/Internet 区域、3G 区域划分为 untrust 区域，公用服务器区域划分为 DMZ 区，其他区域划分为 trust 区域。允许 trust 区域和 DMZ 区域互访，允许 untrust 区域与 DMZ 区域互访，不允许 trust 区域和 untrust 区域之间直接互访。

基于安全考虑，建议 AR 部署 ARP 防攻击功能，接入交换机部署 DHCP Snooping 功能，以防止非法的 ARP 报文对网络的攻击。

4.4.6 远程接入设计

- 中小型机构访问 WAN/Internet 通过 AR 的 NAT 功能实现。
- 外派员工通过 IPSec VPN 访问中小型机构。建议采用 ESP 封装模式，封装新的 IP 报文头并对原始数据报文进行加密，更为安全。

4.4.7 可靠性设计

- 链路备份设计：

  AR 上行采用 WAN 和 3G 链路备份方式，以 WAN 侧链路为主用链路，3G 链路平时不使用，仅作为备份。一旦 WAN 侧链路发生故障，则 AR 自动切换到 3G 链路，从 3G 链路获取公网地址后进行 NAT 转换，实现中小型机构与网络侧的访问。考虑到 WAN 侧链路比 3G 链路安全性高，不受天气影响，WAN 链路带宽也优于 3G 链路，建议当 WAN 侧链路恢复后，采用 AR 自动回切功能，将使用的 3G 链路拆掉，重新切换到 WAN 侧链路。

- 设备备份设计：

  S5700 交换机作为汇聚设备，一旦出现故障将导致所有用户均无法访问网络侧，在中小型机构中建议 S5700 交换机采用堆叠技术，将多台 S5700 交换机虚拟化为 1 台设备，一旦主用 S5700 交换机出现故障后，其他交换机能立即接替其成为主用交换机，确保中小型机构网络业务的正常运行。

4.4.8 网管设计

部署 eSight 网管系统进行日常网络维护。

4.5 中小型机构基础网络方案特点

- 可扩展：低投资、高性能，灵活网络架构，随时扩展语音、无线，保护已有投资。
- 易维护：通过免费网管简单配置，无需专职网管人员。
- 可靠性高：核心汇聚采用堆叠，AR 路由器采用 3G 链路备份，网络层次少，维护简单，可靠性高。

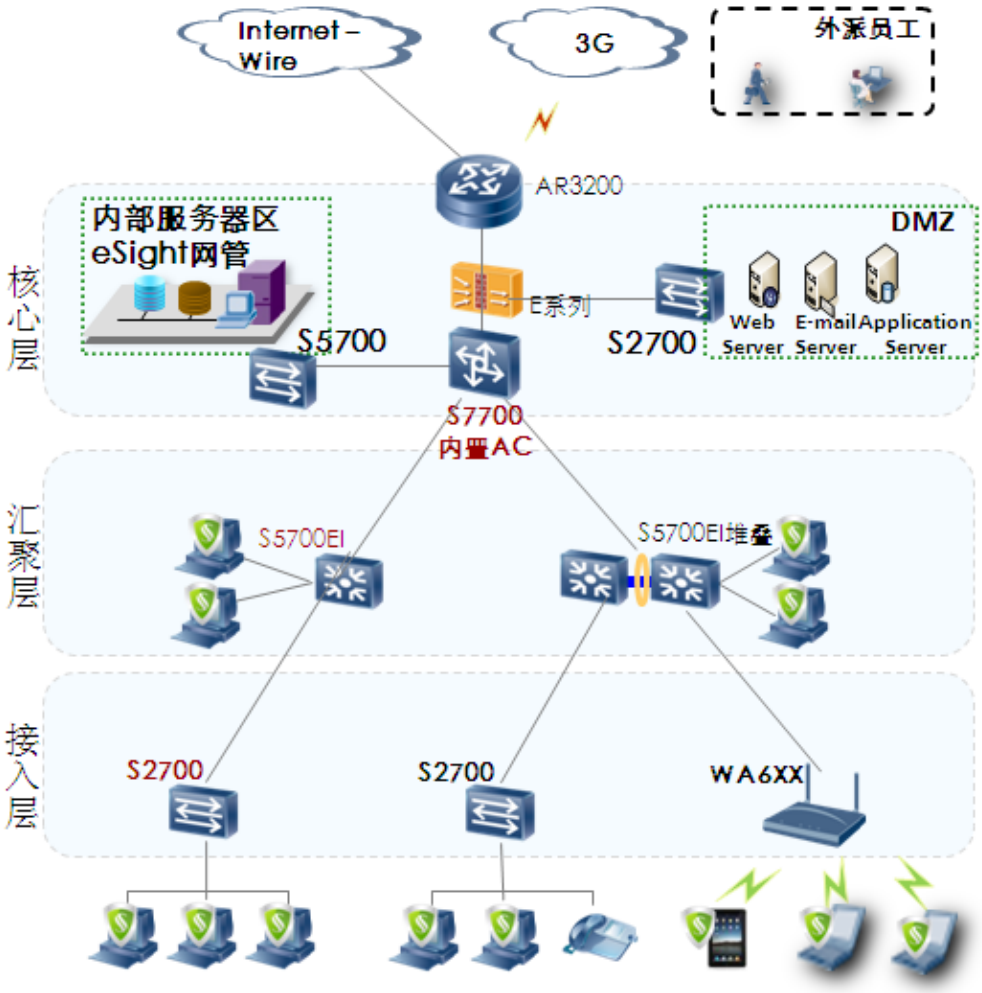
5 中型机构基础网络解决方案

5.1 中型机构基础网络设计原则

中型机构通常为 300～1000 信息点。中型机构基础网络场景的方案特点是期待语音、数据、安全、移动业务丰富，希望获得一体化方案、一站式服务。并且对网络安全要求更高，需要配置专业的防火墙设备提升安全性和远程接入能力。

中型企业的组网结构和中小型企业类似，但因为企业规模的进一步扩大，有更强的企业内部互联以及企业出口的要求，对网络可靠性、可扩展性、安全性的要求更高。这些要求体现在设备上，就是需要功能更强的 AR 作为企业出口路由器、需要专业的防火墙设备、需要通过内置 AC 完成对无线用户的接入控制管理、通过汇聚交换机的双备份以及流量分担。

图5-1 中型机构基础网络物理架构



5.2 中型机构基础网络规划

5.2.1 核心层设计规划

核心层用于转发各部门之间的流量，采用 AR3200 路由器作为核心层出口设备，S7700 系列交换机汇聚内部服务器区、DMZ 区和接入区流量，使内部服务器区、DMZ 区、Internet 区和内部业务区进行互联，支撑内外部的业务流量。核心层部署专业防火墙设备，实现安全防护的同时也作为远程接入 VPN 的网关，实现外派员工与中型机构的互访。

5.2.2 汇聚层设计规划

汇聚层是部门的核心，转发部门用户间的“横向”流量。同时提供到核心层的“纵向”流量。S5700 系列交换机汇聚 S2700 交换机上送的业务流量，用于支撑该汇聚层下各业务部门之间的互访。

5.2.3 接入层设计规划

接入层是最靠近用户的网络，为用户提供各种接入方式，是终端、边缘和 IP 电话等设备接入网络的第一层，一般都部署二层设备。有线用户通过 S2700 交换机接入；无线用户通过 WA600 系列胖 AP 进行无线接入。

5.2.4 出口设计规划

中型机构通过 AR 获取公网地址，实现与 WAN/Internet 的互访，可以采用设置 IP 静态地址或 PPP 动态方式获取公网地址。

5.2.5 可靠性设计规划

AR 上行采用 WAN 和 3G 链路备份方式，以 WAN 侧链路为主用链路，3G 链路平时不使用，仅作为备份。S57 系列交换机采用堆叠技术，将多台 S57 系列交换机虚拟化为 1 台设备，一旦主用 S57 系列交换机出现故障后，其他交换机能立即接替其成为主用交换机。

5.2.6 安全性设计规划

通过 E 系列专业防火墙功能解决如下安全问题：

- 中型机构内、外网之间的访问控制，实现中型机构内、外网的安全隔离。
- 外派员工与中型机构 DMZ 区的访问控制，实现外派员工与内网的安全隔离。

5.3 中型机构基础网络业务方案

5.3.1 数据业务规划

- 有线用户数据业务：

  S2700 交换机作为二层接入设备，通过 VLAN 划分用户。S5700 交换机作为汇聚交换机聚合 S2700 上送的 VLAN 流量，S7700 交换机通过 DHCP 方式为有线用户分配 IP 地址。企业可以根据自身分区情况，划分多个 IP 地址段。S7700 交换机通过静态路由与 AR3200 互通，AR3200 上行通过公网地址接入 WAN/Internet 网络，通过 AR3200 做 NAT，进行私网地址到公网地址的转换，实现有线用户与 WAN/Internet 网络的互访。

- 无线用户数据业务：

  WA600 系列 AP 作为瘦 AP，S7700 交换机内置 AC 板卡，与 WA600 系列 AP 建立 CAPWAP 隧道，无线用户通过 PSK 方式接入 S7700 交换机，S7700 交换机作为三层网关，通过 DHCP 方式为无线用户分配 IP 地址。AR3200 上行通过公网地址接入 WAN/Internet 网络，通过 AR3200 做 NAT，进行私网地址到公网地址的转换，实现无线用户与 WAN/Internet 网络的互访。具体内容请参见 7 中小型机构高级无线解决方案。

- 外派员工数据业务：

  防火墙需要支持 NAT 穿越，AR3200 做 NAT 转换，实现 IPSec VPN 的 NAT 穿越。外派员工通过 IPSec VPN 方式与中型机构的防火墙建立隧道，实现外派员工与中型

机构的互访。可以在外派员工的电脑中安装硬件或通过纯软件方式来实现 IPSec VPN 功能。企业出差用户也可以通过 SSL VPN 方式访问中型机构，可以在防火墙部署 SSL VPN 功能，实现外派员工的访问需求。

- 服务器数据业务：

  企业事先规划好服务器区和 DMZ 的服务器地址，服务器使用静态地址。S2700 交换机作为二层接入设备，通过 VLAN 划分服务器，内部服务器区和 DMZ 区的服务器以 S7700 交换机作为网关。

5.3.2 语音业务规划

基于中型机构人数规模，建议中型机构自行进行控制，AR 作为 PBX 场景应用，用户语音信息到 AR 注册，由 AR 统一分配号码及管理。具体内容请参见 8 中小型机构高级语音解决方案。

5.3.3 安全业务规划

如果需要对用户的接入安全进行控制，则建议部署 NAC 方案。有线用户可以采用在 S2700 交换机上部署 802.1X 认证或者在 S77 系列交换机上部署 Portal 认证的方式，无线用户可以采用在 S77 系列交换机上部署 Portal 认证的方式，均可以实现对用户接入的安全控制，具体内容请参见 6 中小型机构高级安全解决方案。

5.4 中型机构基础网络技术方案

5.4.1 VLAN 设计

VLAN 是将 LAN 内的设备逻辑地而不是物理地划分为一个个网段，从而实现在一个 LAN 内隔离广播域的技术。VLAN 技术既隔离了广播域，减少了广播风暴，又增强了信息的安全性。

- VLAN 通常根据业务需要进行规划，需要隔离的端口配置不同的 VLAN，需要防止广播域过大的地方配置 VLAN 用于减小广播域。
- VLAN 最好不要跨交换机，即使跨交换机数目也需要限制。
- S2700 根据接入位置为不同 PC 分配不同的 VLAN，不同 S2700 交换机采用不同的 VLAN，避免广播域过大，利于问题及时定位。
- S5700 交换机汇聚 S2700 交换机的 VLAN 信息，通过 S7700 系列交换机实现 VLAN 的终结。

5.4.2 IP 设计

IP 地址动态 IP 与静态 IP 的选取，原则上服务器、特殊终端设备建议采用静态 IP。办公用设备建议使用 DHCP 动态获取（如办公用 PC 等）。

AR3200 上行优选固定 IP 地址接入，其次选择 PPP 方式接入。S7700 作为 DHCP 网关和 DHCP Server，为有线、无线用户分配私网 IP 地址。服务器采用静态 IP 地址接入。

5.4.3 DHCP 设计

DHCP 部署基本原则为固定 IP 地址段和动态分配 IP 地址段保持连续，按照业务区域进行 DHCP 地址的划分，便于统一管理及问题定位。启动 DHCP 安全功能，禁止非法 DHCP Server 的架设和非法用户的接入。

有线用户通过 S2700 交换机携带 VLAN 信息，S7700 交换机作为 DHCP 网关和 DHCP Server，S7700 交换机终结 VLAN 并给有线用户分配私网 IP 地址。无线用户通过 CAPWAP 隧道方式接入 S7700 交换机。WA600 系列 AP 终结无线报文，通过 CAPWAP 隧道透传无线用户的 DHCP 请求报文，S7700 交换机终结该请求报文，给无线用户分配私网 IP 地址。

5.4.4 NAT 设计

NAT 称为网络地址转换，用于实现私有网络和公有网络之间的互访。AR3200 部署 NAT 特性，实现用户侧私网地址到网络侧公网地址的转换，实现用户与 WAN/Internet 的互访。在中型机构基础网络场景中，WAN 侧和 3G 侧都需要部署 NAT 特性，以防止某侧链路出现故障后仍能实现私网地址到公网地址的转换。

5.4.5 安全设计

防火墙 E1000E 将 WAN/Internet 区域、3G 区域划分为 untrust 区域，公用服务器区域划分为 DMZ 区，其他区域划分为 trust 区域。允许 trust 区域和 DMZ 区域互访，允许 untrust 区域与 DMZ 区域互访，不允许 trust 区域和 untrust 区域之间直接互访。

基于安全考虑，建议防火墙部署 ARP 防攻击功能，接入交换机部署 DHCP Snooping 功能，以防止非法的 ARP 报文对网络的攻击。

5.4.6 远程接入设计

中型机构访问 WAN/Internet 通过 AR 的 NAT 功能实现。外派员工通过 IPSec VPN 访问中型机构。建议采用 ESP 封装模式，封装新的 IP 报文头并对原始数据报文进行加密，更为安全。外派员工也可以通过 SSL VPN 访问中型机构。

5.4.7 可靠性设计

- 链路备份设计：

  AR 上行采用 WAN 和 3G 链路备份方式，以 WAN 侧链路为主用链路，3G 链路平时不使用，仅作为备份。一旦 WAN 侧链路发生故障，则 AR 自动切换到 3G 链路，从 3G 链路获取公网地址后进行 NAT 转换，实现中型机构与网络侧的访问。考虑到 WAN 侧链路比 3G 链路安全性高，不受天气影响，WAN 链路带宽也优于 3G 链路，建议当 WAN 侧链路恢复后，采用 AR 自动回切功能，将使用的 3G 链路拆掉，重新切换到 WAN 侧链路。

- 设备备份设计：

  S5700 交换机作为汇聚设备，一旦出现故障将导致所有用户均无法访问网络侧，在中型机构中建议 S5700 交换机采用堆叠技术，将多台 S5700 交换机虚拟化为 1 台设备，一旦主用 S5700 交换机出现故障后，其他交换机能立即接替其成为主用交换机，确保中型机构网络业务的正常运行。

5.4.8 网管设计

部署 eSight 网管系统进行日常网络维护。

5.5 中型机构基础网络方案特点

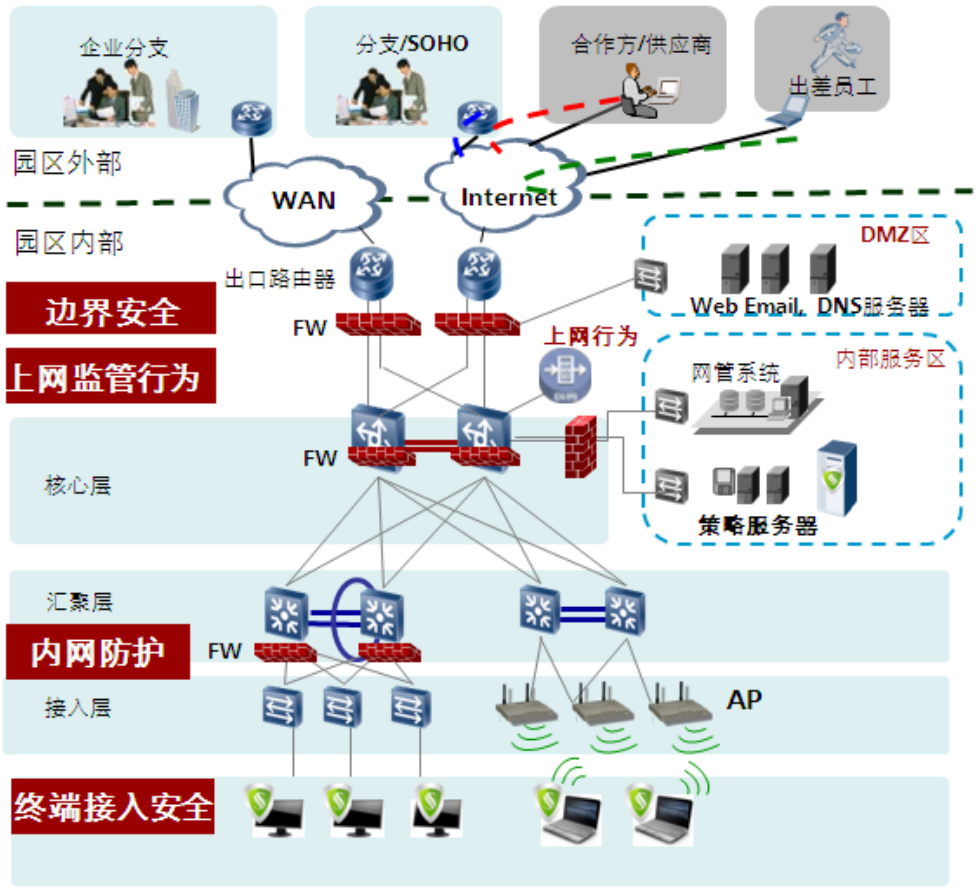
- 有线无线一体化：内置 AC，有线无线统一调度，节省投资。
- 可扩展：低投资、高性能，灵活网络架构，随时扩展语音、无线业务，保护已有投资。
- 易维护：通过网管简单配置，无需专职网管人员。
- 可靠性高：核心汇聚采用堆叠，AR 路由器采用 3G 链路备份，网络层次少，维护简单。

6 中小型机构高级安全解决方案

6.1 中小型机构高级安全设计原则

中小企业通常为 100～1000 信息点，通过部署高级安全解决方案实现网络安全一体化。该方案特点是通过部署 NAC 解决方案实现有线、无线用户的一体化接入安全控制，包括安全准入、终端检查、权限控制及事后审计功能，实现全面的安全控制，确保企业网络的安全性。

图6-1 中小型机构高级安全物理架构



6.2 中小型机构高级安全业务方案

6.2.1 园区用户接入安全业务规划

在中小型及中型园区中，关于有线用户接入认证推荐两种方案：接入层、汇聚层动态授权方案和核心层 Portal 方案。

接入层动态授权方案使用 S2700/S3700/S5700 系列交换机作为接入交换机，S5700 或 S7700 交换机作为汇聚交换机。接入层使用 VLAN 划分用户的所属部门，使用 802.1x 认证技术根据端口进行认证；用户认证前统一在 Guest VLAN 里进行授权，用户认证后，由认证服务器下发 VLAN 进行部门划分；核心交换机作为网关，使用 DHCP 动态分配 IP 地址，根据认证前后所属 VLAN 配置 ACL 权限，对用户部门进行权限限制，并接入内网进行访问。汇聚层交换机使用 VRRP 功能进行主备备份，提高网络可靠性。

核心层 Portal 方案同样使用 S2700/S3700/S5700 系列交换机作为接入交换机，S5700 或 S7700 交换机作为汇聚交换机。接入层交换机作为二层透传设备，为接入用户划分 VLAN。核心交换机作为网关，启用 DHCP 动态分配 IP 地址，使用华为 Portal 协议进行网关认证；用户认证前使用 Freerule 功能为用户进行认证前权限限制，认证后用户的具体权限由认证服务器以 ACL 形式进行权限下发，并接入内网进行访问；无线用户接入认证，推荐采用核心层 S7700 交换机内置 AC 方式认证。使用核心层内置 AC 设备认证的时候，接入层交换机下挂 AP，采用独立模式或集中模式认证；接入层交换机配置二层透传，透传 AP 发出的报文，核心层交换机使用 DHCP 进行 IP 地址分配，并由内置 AC 进行认证。

6.2.2 远程分支用户接入安全业务规划

分支用户分为小型分支、中型分支、大型分支企业。

小型分支接入点数目一般在 100 个左右，推荐采用在分支出口路由器 AR 设备上启用 Portal 认证，使用户在企业出口强制进行认证和安全状态检查。如果终端包含语音设备，还需要在 AR 设备上启用 MAC 认证；小型分支建议 AR 作为网关，使用 DHCP 动态为接入用户分配 IP 地址。此时认证服务器建议部署在分支，并将数据同步到总部服务器；也可以采用在汇聚交换机设备上启用网关做 Portal 认证，使用户在网关进行认证和安全状态检查。根据终端设备类型启用 MAC 认证。网关使用 DHCP 动态为接入用户分配 IP 地址。此时认证服务器可以部署在总部，分支网络与总部网络使用通过出口路由器以 IPSec VPN 方式与总部 AR 建立隧道，实现分支企业与总部的互访。

企业中型分支接入点在 100 以上，1000 以下，认证服务器一般根据分支用户规格选择性的部署在分支内部或者使用总部的认证服务器。中型分支网络核心层作为网关动态分配 IP 地址。用户接入方式可同园区一样使用在分支接入层交换机采用 802.1x 认证或 MAC 认证方案或在核心层配置 Portal 认证方案。用户认证后由认证服务器根据认证方式下发权限，用户可接入分支内部访问网络，也可通过 AR 访问总部网络。分支网络与总部网络使用通过出口路由器以 IPSec VPN 方式与总部 AR 建立隧道，实现分支企业与总部的互访。

企业大型分支接入点在 1000 以上，在分支网络中，认证服务器一般部署在分支内部。认证方式与中型分支一样，在此不赘述。

6.2.3 边界安全业务规划

在企业互联网出口部署防火墙及 VPN 设备，分支机构及移动办公用户分别通过 VPN 网关（AR 设备）和 VPN 客户端安全连入企业内部网络。同时通过防火墙将企业内部网、DMZ、数据中心、互联网等安全区域分隔开。

在核心交换机与 Internet 路由器之间配置两台防火墙，两台防火墙与核心交换机以及 Internet 路由器之间采取全冗余连接，保证系统的可靠性，建议配置两台防火墙为双机热备方式，在实现安全控制同时保证线路的可靠性，同时可以与内网动态路由策略组合，实现流量负载分担。配置防火墙全面安全防范能力，通过防火墙的访问控制策略，控制来自 Internet 用户只能访问 DMZ 区服务器的特定端口，对内部用户访问 Internet 进行基于 IP 地址的控制。

VPN 网关部署在园区边界，IPSec VPN 的方式除为出差员工提供随时随地的接入功能，同时提供企业分支和总部的一对一的 VPN 功能。

推荐使用华赛 USG 统一网关产品，USG 接口类型丰富，接口密度大，提供固定、移动、无线统一接入，提供家庭、企业、热点统一接入，最大程度满足了用户的多种接入需求，并且支持多种路由交换协议，可满足中小型企业、大中型企业的分支机构、行业网的分支机构以及部分电信网络的需求。同时 USG 拥有强大的安全防护能力、增强的报文过滤功能、状态检测安全功能、黑名单过滤恶意主机、IP 和 MAC 地址绑定、强大的防攻击功能，并支持 VPN 特性。

6.2.4 内网审计业务规划

园区用户上网行为审计业务，推荐使用 SINFOR AC 串行在园区网中进行上网行为管理。实现对用户行为的识别、访问控制和监控审计。

SINFOR AC 可以采用网桥模式，串接在接入层交换机和汇聚层交换机之间，对所有流经 AC 的数据流进行审计，管理和控制。当 AC 出现策略或者设备故障问题时，AC 将成为一条透明的网线，放行所有的数据，不影响组织的正常上网。

6.3 中小型机构高级安全技术方案

6.3.1 安全检查设计

终端必须在安全的状态才能接入网络，华赛 TSM 拥有丰富的安全策略，可以实现对终端的安全检查。不但可以对入网终端的安全性（杀毒软件安装、补丁更新、密码强度、屏保等）进行扫描，在接入网络前完成终端安全状态的检查；同时对终端不安全状态能够与控制设备进行联动，当发现不安全终端接入网络的时候，能够对这些终端实现一定程度的阻断，防止这些终端对业务系统的危害，并能够主动帮助这些终端完成安全状态的自修复；对于未能及时修复的不安全终端，能够对其进行权限限制，避免接入网络，引发网络安全问题。

6.3.2 远程接入安全设计

分支机构通过 IPSec VPN 方式访问总部，建议采用隧道模式，封装新的 IP 报文头并对原始数据报文进行加密，更为安全。

机构访问 WAN/Internet 则通过 AR 的 NAT 功能实现。

外派员工及微型机构用户使用客户端，通过 IPSec VPN 访问总部。

6.3.3 防火墙设计

为了能够有效的阻挡来自 Internet 上的攻击，保护企业在 Internet 边界部署的服务器，使之提供公众访问功能的同时，还能够保护这些服务器的安全。推荐在核心交换机与 Internet 路由器之间配置两台防火墙，两台防火墙与核心交换机以及 Internet 路由器之间采取全冗余连接，保证系统的可靠性，建议配置两台防火墙为双机热备方式，在实现安全控制同时保证线路的可靠性。

同时可以与内网动态路由策略组合，实现流量负载分担。配置防火墙全面安全防范能力，通过防火墙的访问控制策略，控制来自 Internet 用户只能访问 DMZ 区服务器的特定端口，对内部用户访问 Internet 进行基于 IP 地址的控制。

6.3.4 内网安全设计

企业对于来自 Internet 的威胁可以通过部署防火墙达到保护局域网的内部用户免受蠕虫、间谍软件的侵扰，实现安全上网。而对于局域网内部计算机客户端的安全威胁，除了使用终端准入控制技术，也可以在网络设备上配置相关防攻击特性，实现网络安全的保护。

目前对于内网威胁，可以考虑在核心层，汇聚层，接入层分别部署不同特性。如在接入层部署 MFF 功能，防止用户非法互访；通过在接入层配置 MAC 限速，防止 MAC 泛洪；在汇聚层配置 IP Souce Gurad 来防止 IP 欺骗，也可以考虑配置 DHCP 限速防止 DHCP 泛洪。

6.3.5 内网审计设计

SINFOR AC 以串联的方式接在路由设备和交换设备之间，即防火墙/路由器和交换机中间。不做 NAT 和选路，但对所有经过的应用流量都具有控制功能。AC 具有开机 BYPASS、软件 BYPASS 和硬件 BYPASS 功能，当 AC 出现策略或者设备故障问题时，AC 将成为一条透明的网线，放行所有的数据，不影响组织的正常上网。

由于网桥模式不需要更改组织的网络结构，只需一个 IP 地址，管理员就可以管理内网。

6.3.6 ARP 防攻击设计

由于 ARP 攻击利用的是网络协议漏洞，所以可以通过攻击、病毒、木马等多种形式发起，这种攻击难以从源头上消灭。最好的办法就是将 ARP 攻击限制在尽可能小的范围内，以达到防御 ARP 攻击的目的。

ARP 攻击防御可以在网关层、接入层和终端进行，在接入层和终端部署效果最好。

- 在网关层，部署 ARP 严格学习或部署 ARP 防 IP 攻击功能来阻止 ARP 仿冒网关攻击；在网关配置 APR 源抑制功能，来防止 APR 泛洪攻击，这部分功能也可以部署在防火墙上。
- 在接入层，可部署 DHCP Snooping 功能丢弃非法入侵的 ARP 报文。

- 同时在部署 TSM 认证系统的终端 PC 上启用 TSM 的 ARP 保护功能，可防止本机发起的 ARP 欺骗攻击和 ARP 泛洪攻击，也可通过 IP 与 MAC 的绑定防止主机遭受 ARP 攻击。

华为公司提供多种 ARP 防御方案，针对不同的企业应用和需求，能够灵活选择最适合企业的 ARP 防御方案；能够从源头堵截 ARP 攻击，更高效的防御 APR 攻击。

6.4 中小型机构高级安全方案特点

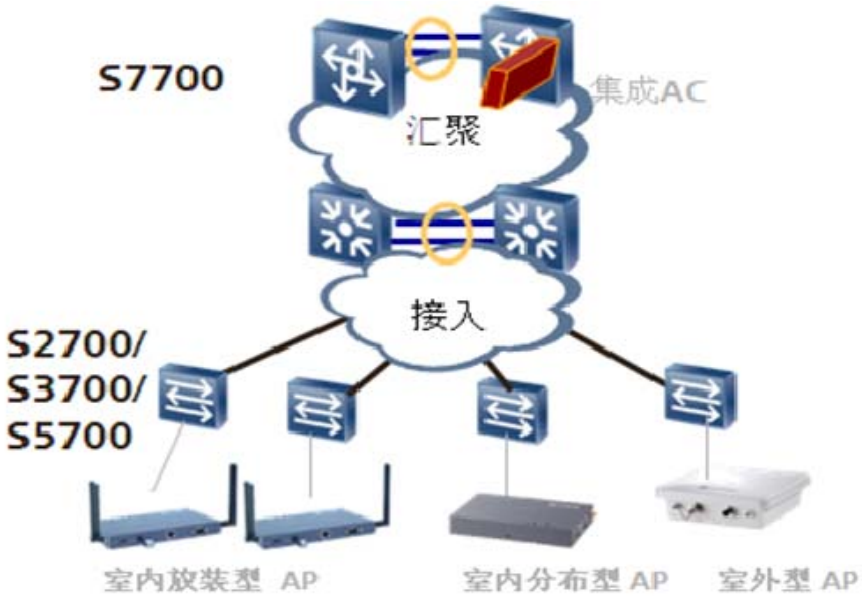
- 接入安全：NAC 方案提供完善的接入、检查、访问控制和审计功能，接入更安全。
- 一体化管理：有线无线一体化接入控制，管理更简单。
- 防范 ARP 攻击：网络设备提供完善的 ARP 攻击防范措施，TSM 客户端自动实现 IP 与 MAC 绑定，防止主机中病毒后的主动攻击行为，确保网络安全可靠。

7 中小型机构高级无线解决方案

7.1 中小型机构高级无线设计原则

中小型机构和中型机构无线信息点通常含有 100～1000 信息点，主要场景为咖啡厅、商业酒店、展厅与证卷大厅、体育场馆新闻中心、制造车间、物流运输。该方案特点是支持多种无线终端的安全接入，对无线高优先级业务进行 QoS 保证，实现有线无线的一体化应用，减少企业的运维成本。

图7-1 中小型机构高级无线物理架构



7.2 中小型机构高级无线业务方案

7.2.1 无线用户接入业务规划

- 通过 PSK 方式接入无线网络：

S7700 部署 AC 板卡，无线用户通过 PSK 方式接入 S7700，S7700 作为三层网关，通过 DHCP 方式为无线用户分配 IP 地址。

- 通过 802.1X 方式接入无线网络：

  企业如果需要对用户进行精细化控制和管理，则建议在服务器区部署 AAA 服务器。区域内用户通过在 AC 上部署 802.1X 认证方式对接入用户进行身份认证，认证通过后由 AC 作为三层网关并为无线用户分配 IP 地址。

- 通过 Portal 方式接入无线网络：

  对于外来访客等接入无线网络，建议使用 Portal 方式，Portal 认证可结合 WLAN 终端身份验证来完成 WLAN 用户的接入认证以及加密。在 AC 上使能 Portal 认证功能，认证通过后可以访问 WAN/Internet 网络。该方案不需要安装客户端软件，安全性相比于 802.1X 认证较差。

7.2.2 无线语音终端用户接入业务规划

无线语音终端通过 MAC 认证方式接入无线网络，AR 可以作为 PBX 设备对该无线电话终端进行注册，或者 AR 作为 AG 设备将该无线语音终端的注册信息送到总部的 PBX 上进行注册，最终完成语音业务。具体内容请参见 8 中小型机构高级语音解决方案。

7.2.3 有线无线一体化接入业务规划

中小企业建议通过一套系统完成有线无线用户的统一接入，利于网络规划的同时也利于统一管理。802.1X 认证需要安装客户端并且部署在不同的接入交换机上，不利于统一维护管理。建议通过在网关设备上部署统一的 Portal 认证机制，实现有线无线的一体化接入。

7.3 中小型机构高级无线技术方案

7.3.1 WLAN 认证设计

相对于简单的 WLAN 终端身份验证机制，用户身份验证的安全性大大提高。通过提供有限的访问权限来验证用户身份，只有确定用户身份后才给予完整的网络访问权限，可有效判别用户的合法性。

WLAN 用户身份验证主要有 Portal、PSK、802.1X 等几种认证方式：

- PSK 认证需要实现在客户端和设备端配置相同的预共享密钥，而具体的认证过程实际上在密钥协商过程（EAPOL-Key 密钥协商过程）中完成。
- Portal 认证由于认证过程中不会协商 WLAN 用户空口所需的加密密钥，因此 Portal 认证可结合 WLAN 终端身份验证来完成 WLAN 用户的接入认证以及加密。
- 802.1X，支持的认证类型有：EAP-TLS、EAP-PEAP、EAP-MD5、EAP-PAP，其中 EAP-MD5、EAP-PAP 支持本地认证。

中小企业中无线用户接入认证部署方式建议如下：

表7-1 无线用户接入认证方式比较

认证方式	优点	劣势	适用场景
802.1x(EAP-TLS、EAP-PEAP)	1、安全性高 2、PC 终端普遍支持	1、需安装客户端软件 2、采用 EAP-TLS 认证时网络部署难度大	企业，且网络中部署了认证服务器。
Portal+PSK	不需要安装客户端软件	安全性较差	校园网、企业访客用户等，网络中部署了认证服务器。
Portal+开放系统认证	不需要安装客户端软件	安全性较差	企业访客用户等，网络中部署了认证服务器。
PSK	1、不需安装客户端 2、网络不需部署认证服务器，降低部署成本	安全性较差	没有部署认证服务器的网络。

7.3.2 SSID 与 VLAN 设计

中小企业可以使用一个 SSID，给所有人员提供 WLAN 接入服务；如需要划分不同 SSID 便于中小企业管理，则可以使用多个 SSID，多个 SSID 可以映射到相同 VLAN 或者不同 VLAN。

业务 VLAN 用于区分不同的业务群体，在 WLAN 中 SSID 也可以承担相应的功能，因此可以综合考虑 VLAN 与 SSID 的映射关系。

- SSID:VLAN=1:1，企业希望员工搜到的 WLAN 只有一个 SSID，并且给员工分配同一网段的地址，则 VLAN 只需要规划一个，例如 VLAN 100。
- SSID:VLAN=N:1，中小企业希望员工根据搜到的多个 SSID 进行选择接入，但是希望给员工都分配同一网段的地址，则 VLAN 也只需要规划一个，例如 VLAN 100。
- SSID:VLAN=1:N，中小企业有多个胖 AP 分布在不同区域，企业希望员工搜到的 WLAN 只有一个 SSID，但是希望根据不同区域给用户分不同网段的地址加以区分，则 VLAN 需要规划多个，例如 VLAN 100、VLAN 200。
- SSID:VLAN=N:N，中小企业希望员工根据搜到的多个 SSID 进行选择接入，并且希望给员工分配不同网段的地址，则 VLAN 需要规划多个，例如 VLAN 100，VLAN 200。

中小企业可以根据自身业务需要，从上述四种方式中任选其一，完成企业 VLAN 的规划部署。

7.3.3 DHCP 设计

DHCP 部署基本原则为固定 IP 地址段和动态分配 IP 地址段保持连续，按照业务区域进行 DHCP 地址的划分，便于统一管理及问题定位。启动 DHCP 安全功能，禁止非法 DHCP Server 的架设和非法用户的接入。

无线用户通过 CAPWAP 隧道方式接入 S7700 交换机。AP 终结无线报文，通过 CAPWAP 隧道透传无线用户的 DHCP 请求报文，S7700 交换机终结该请求报文，给无线用户分配私网 IP 地址。

7.3.4 射频设计

- 射频信道选择：

  对于无线局域网，信道是非常稀缺的资源，例如对于 2.4G 网络，只有 3 个非重叠信道，智能的分配信道是无线应用的关键。同时，无线局域网工作的频段存在大量可能的干扰源，如雷达、微波等，它们将干扰 AP 的正常工作。通过信道调整功能，可以保证每个 AP 能够分配到最优的信道，尽可能地减少和避免相邻信道干扰。动态信道调整能够实现通信的持续进行，为网络的可靠传输提供保证。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。

- 射频功率选择：

  传统的射频功率控制方法只是静态地将发射功率设置为最大值，单纯地追求信号覆盖范围，但是功率过大可能导致对其他无线设备造成不必要的干扰。因此，需要选择一个能平衡覆盖范围和系统容量的最佳功率。AP 支持手动和自动两种方式设置射频功率。一旦检测到冲突后会进行功率调整，实现动态的分配合理的功率。

- 射频速率选择：

  802.11 在发展的过程中出现了不同的标准：802.11 a/b/d/e/f/g/h/i/j/k/n/p/r/s/t/u。其中 802.11a、802.11b、802.11g、802.11n 这些属于物理层标准，即我们所谓的射频类型。不同的物理层标准，决定了射频在单位时间内可以装载不同容量的数据，即射频的速率。我们可配置射频的速率模式为指定或自动，指定的速率或自动模式时的最大速率必须在射频类型支持的速率集内。目前 AP 一般支持多种射频类型，推荐中小企业选择 802.11g 或 802.11n 模式，其中 802.11g 模式最大射频速率为 54M，802.11n 最大射频速率理论可以达到 600M。

- 射频补盲：

  当某些 AP 下线或故障时，就需要调大周围邻居的功率进行补盲。当一台 AP 下线或出现故障时，邻居 AP 检测到信道功率后自动调节 AP 的发射功率，增强 AP 的下行信号，从而达到补盲的效果。建议 AP 使能射频补盲功能。

7.3.5 WMM 设计

WMM 按照优先级从高到低的顺序分为 AC-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。

Priority	UP (Same as 802.1D user priority)	802.1D designation	AC	Designation (informative)
Lowest	1	BK	AC_BK	Background
	2	—	AC_BK	Background
	0	BE	AC_BE	Best Effort
	3	EE	AC_BE	Best Effort
	4	CL	AC_VI	Video
	5	VI	AC_VI	Video
	6	VO	AC_VO	Voice
Highest	7	NC	AC_VO	Voice

基于上述因为业务层面不同而产生的不同应用需求，我们推荐根据需要在不同 AP 上制定不同的 WMM 策略，某些 AP 提高语音和视频的优先级，某些 AP 提高数据转发的优先级。

7.3.6 频点设计

基于 IEEE802.11 系列标准的 WiFi 拥有 2.4GHz 和 5GHz 两个频段，其中 2.4GHz 频段可选信道有 14 个，每个信道带宽为 22MHz，只有 3 个信道相互之间无干扰，我国选用 1、6、11 等三个信道；5GHz 频段可选信道为 24 个，我国选用 149、153、157、161 及 165 等五个信道。

说明

需要注意的是，不同的国家或地区使用的信道或频段是不同的，在实际规划中需要事先了解具体要求。

图7-2 2.4G 频段信道划分

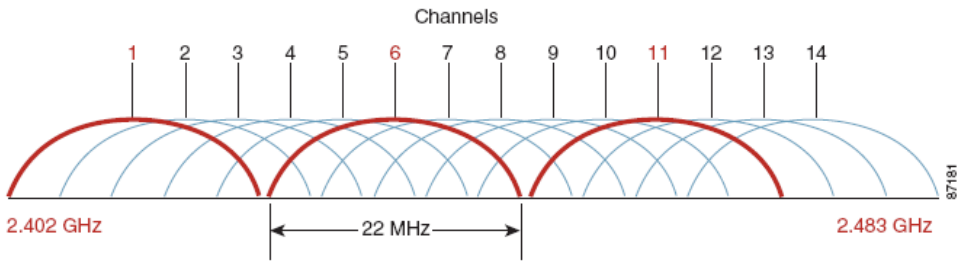


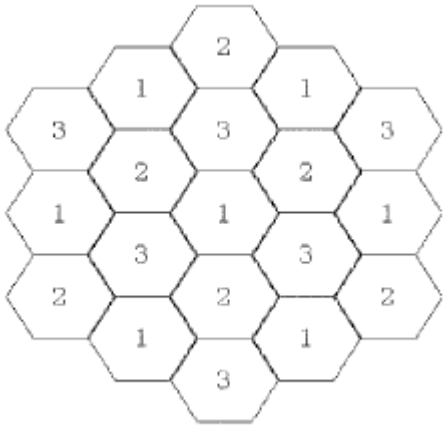
图7-3 2.4G 频段信道各地区应用

Channel Identifier	Center Frequency	FCC (America)	ESTI (EMEA)	TELEC (Japan)	MOC (Israel Outdoor)[1]
1	2412	X	X	X	
2	2417	X	X	X	
3	2422	X	X	X	
4	2427	X	X	X	
5	2432	X	X	X	X
6	2437	X	X	X	X
7	2442	X	X	X	X
8	2447	X	X	X	X
9	2452	X	X	X	X
10	2457	X	X	X	X
11	2462	X	X	X	X
12	2467		X	X	X
13	2472		X	X	X
14	2484			X	

在 WLAN 的工程部署中，往往需要多个 AP，如果不同的 AP 工作在相同的频道，就可能形成同频干扰。为保证频道之间不相互干扰，在多个频道同时工作的情况下，就要求两个频道的中心频率间隔不能低于 25MHz。

为了扩大覆盖范围和提高频谱利用率，WLAN 也需要引入蜂窝结构，对于 1、6 和 11 三个信道交错使用，具体的覆盖示意图如下（1：代表信道 1、2：代表信道 6、3：代表信道 11）：

图7-4 信道规划示意图



7.3.7 覆盖设计

通过现场勘测确定站点的基本情况，了解建筑周围的传播环境，以明确选用何种部署方式（室内放装、室内分布和室外覆盖）、各区域的用途，帮助工程师确定容量、覆盖和

业务质量要求，避免图上作业的局限。站点勘测可以帮助确定 AP、天线安装位置，以及走线路由。

根据勘查计划，进行站点无线勘测。勘测过程中需要记录以下信息：周围无线传播环境条件（照片）、建筑空间分割等的现场查看、可能的 AP 安装位置、弱电井可能走线位置。

另外勘测中需要询问各空间的用途，判断话务类型、高峰时间。另外注意电梯、出入口人员移动路线。帮助确定容量、切换区的设置。

覆盖预测过程和无线站址勘测过程是紧密关联的。在网络规划过程中，覆盖预测通常并不是一次就可以达到网络规划目标，需要进行若干次的反复调整。预测的主要内容包括：输入数据采集，预测工作，预测报告。

7.3.8 链路预算设计

链路预算（link budget），是在一个通信系统中对发送段、通信链路、传播环境（大气、同轴电缆、波导、光纤等）和接收端中所有增益和衰减的核算。其通常用来估算信号能成功从发射端传送到接收端之间的最远距离。

WLAN 链路预算一般经过以下步骤：

1. 确定边缘场强：一般地，在 WLAN 工程部署中，要求重点覆盖区域内的 WLAN 信号到达用户终端的信号强度不低于－75dBm。
2. 分析传输模型，确定空间传播损耗公式：

   对接收电平的估算通常采用如下公式：

   $$Pr[dB] = Pt[dB] + Gt[dB] - Pl[dB] + Gr[dB]$$

   其中：Pr[dB]为最小接收电平，即为 AP 在不同传输速率下的接收灵敏度；Pt[dB]为最大发射功率；Gt[dB]为发射天线增益；Gr[dB]为接收天线增益；Pl[dB]为路径损耗（包括空间传播损耗、馈线传播损耗、墙体/玻璃阻挡损耗）。
3. 确定空间传播损耗：

   实际部署中终端天线增益不可知，为方便计算常忽略接收天线增益，而采用如下公式：

   到达用户端的信号电平＝AP 发射功率＋AP 天线增益－路径损耗

   路径损耗包括：

   - AP 到天线间的馈线损耗：适用于室内分布式部署，在室外部署时如果馈线过长也需考虑。
   - WLAN 信号的空间损耗：适用于所有部署方式，根据电磁波空间衰减公式计算。

     空间损耗＝92.4+20lgf+20lgd（f：GHz，d：km）

     由公式推算可知：

空间传输距离(m)	100	200	300	400	500	600	1000
2.4GHz 信号的空间衰减(dBm)	80	86	89.5	92	94	95.5	100
5.8GHz 信号的空间衰减(dBm)	87.6	93.6	97.1	99.6	101.6	103.1	107.6

   - 墙体/玻璃阻挡：适用于所有部署方式，一般根据经验值判定。

2.4GHz 电磁波对于各种建筑材质的穿透损耗的经验值如下：钢筋混凝土墙 20-30dB；木制家具、门和其它木板隔墙阻挡 2-15dB；厚玻璃（12mm）10dB。

4. 根据公式计算覆盖距离，判断是否满足覆盖要求：

为便于理解链路估算的过程，这里给出一个室外场地覆盖的预算案例。

根据 WLAN 覆盖边缘场强的要求，到达终端用户的信号电平不低于－75dBm，500mW AP 的输出电平 27dBm，天线增益 9dBi，距离 AP 500m 时信号的衰减量 94dBm，可知：

27+9-94＝-58dBm，大于-75dBm，

因此在正常情况下，AP 可以为 500M 处用户可以提供满速率接入。

----结束

7.3.9 容量设计

WLAN 的 AP 设备允许多个用户同时接入，但如果接入用户数目过多，会导致用户体验下降，因此建议一般每个 AP 接入的用户数量控制在 20～30 之间为宜。

7.4 中小型机构高级无线方案特点

- 全新的 802.11n 网络，完全兼容原有的 802.11 a/b/g 用户接入。
- 支持最大 600M 带宽，当前 300M 带宽。
- 核心交换机一体化集成的 AC 配合多种类 AP 满足各种场景的覆盖需求。
- 交换机提供 PoE 功能，为 AP 供电。

8 中小型机构高级语音解决方案

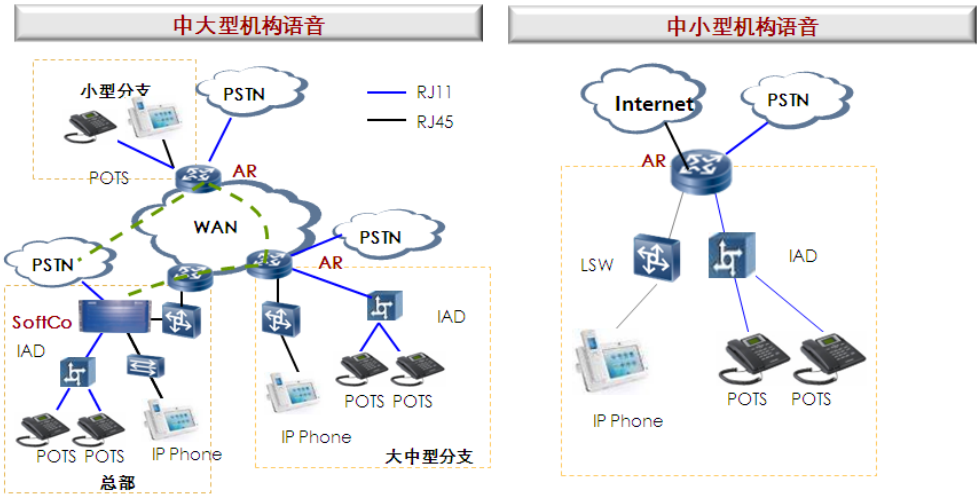
8.1 中小型机构高级语音设计原则

中小型机构通常含有 100～1000 信息点，对 IP 语音提供丰富业务，低资费的特点感兴趣。目前大多数企业的各分支机构之间的电话通信都是通过 PSTN 网络实现的，巨额话费已经成为许多企业的沉重负担。因此经济实惠的电话网络解决方案已经成为许多企业的迫切需求。

VoIP 则是这一问题的最佳解决方案。与普通电话相比，IP 电话的优势是非常明显的，因为 IP 电话将电话网络整合到数据网络中，省去了庞大的 PSTN 长途话费开支，可以显著降低企业网络的运营成本。

华为语音解决方案包含一系列智能、简便、安全和综合化的产品、服务专为中小型企业设计，能够帮助企业控制成本、对竞争压力做出迅速反应并提升经营效率。这一行业领先的解决方案能够统一企业中所有通信及商业过程，为企业增加强势支持和完全可管理的 IP 语音及数据网络服务，使企业能够专注于企业的核心竞争力，增强经营能力，壮大企业发展。

图8-1 中小型机构高级语音物理架构



8.2 中小型机构高级语音业务方案

8.2.1 中型机构分布式多分支语音业务规划

中大型机构分布式多分支呼叫控制部署：总部以及各个分支的出口语音设备分别部署 IP PBX。总部采用 SoftCo 设备充当 IP PBX，可以提供丰富的补充业务；分支采用 AR 设备，既充当出口路由器，又充当分支 IP PBX 功能。各分支和总部的语音用户在本地完成用户注册和呼叫控制，总部 IP PBX 为各个分支互通提供呼叫路由，形成总部为一级呼叫路由，分支为二级呼叫路由的结构。IP PBX 设备下挂 IAD 设备，一方面扩大了接入用户数量，另外一方面提供了 POST 话机的接入方式，实现模拟信号到数字信号的转换。总部和分支 IP PBX 设备分别接入当地运营商网络，可以是 IMS 或者 PSTN。企业可以为分散在不同城市的办公分支提供 VoIP 服务，不同分支间可使用企业短号进行通话以及企业对分支所在地的外线呼叫，可通过 IP 网络承载，节省企业的长途语音通信费用。

8.2.2 小型机构分布式多分支语音业务规划

中小型机构由于分支少，语音用户数量规模不大，建议总部以及各个分支部署 AR 作为出口路由器，并且兼顾 IP PBX 功能。各分支和总部的语音用户在本地完成注册和呼叫控制。总部和各分支之间一般通过 IPSec VPN 实现互联。总部 IP PBX 为各个分支互通提供呼叫路由，形成总部为一级呼叫路由，分支为二级呼叫路由的结构。IP PBX 设备下挂 IAD 设备，一方面扩大了接入用户数量，另外一方面提供了 POST 话机的接入方式，实现模拟信号到数字信号的转换。总部和分支 IP PBX 设备分别接入当地运营商网络，可以是 IMS 或者 PSTN。企业可以为分散在不同城市的办公分支提供 VoIP 服务，不同分支间可使用企业短号进行通话以及企业对分支所在地的外线呼叫，可通过 IP 网络承载，节省企业的长途通信费用。

8.3 中小型机构高级语音技术方案

8.3.1 终端接入设计

语音接入终端包括：POTS 话机、IP 电话、PC 软终端、传真机。各种不同的语音终端的接入方式如下：

- 模拟电话接入方式

  模拟电话通过 FXS 线路直接接到 IP PBX 设备下；

  模拟电话通过 FXS 线路接到 IAD 设备，IAD 设备通过以太链路接到 IP PBX 设备下。
- IP 电话接入方式

  IP 电话通过接入用户的 LAN 网络后，注册到 IP PBX 设备下。
- PC 软终端接入方式

  PC 软终端通过接入用户的 LAN 网络后，注册到 IP PBX 设备下。
- 传真机接入方式

  传真机通过 FXS 线路直接接到 IP PBX 设备下；

  传真机通过 FXS 线路接到 IAD 设备，IAD 设备通过以太链路接到 IP PBX 设备下。

一般情况下，由于 AR 接口数量限制，用户终端设备均通过 IAD 设备接入到 IP PBX。

IP 电话终端、各 IAD 的 IP 地址建议同本地的 IP PBX 保持在同一网段。终端 IP 的分配方式有两种手段：

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

8.3.2 网络接入设计

IP PBX 上面需要配置语音中继，以实现和其他 IP PBX、运营商网络的对接。常用的中继类型有：AT0、PRA、SIPAT0、SIPIP。

表8-1 语音中继的分类和用途

中继类型	描述	用途
AT0	使用RJ11电缆接入运营商网络，提供1路语音	接入PSTN网络
PRA	使用E1电缆接入运营商网络，提供最多30路语音	接入PSTN网络
SIPAT0	使用RJ45通过WAN接入运营商，提供1路语音	接入IMS网络
SIPIP	使用RJ45通过以太网和其他SIPIP中继对接	和SIPIP中继对接

企业根据自身的需要可以选择上述不同的中继接入方式接入运营商网络。一般推荐使用 E1 线路的 PRA 方式接入 PSTN 网络。

企业分支也部署了 IP PBX。除了要在各分支的 IP PBX 上面配置接入运营商网络的中继之外，还需要在各分支 IP PBX 上配置分支之间的 SIPIP 中继，以实现分支之间的 VoIP 通话。

对于分支之间的中继配置，可以部署总部集中转发方式，分支之间的语音信令流均通过总部实现互通。这样做的好处是如果分支较多时可以统一管理，简化配置，降低维护成本；另外当新增一分支时，只需修改总部和新增分支的配置即可实现各分支语音互通。

8.3.3 号码规划设计

若需要内部用户短号与出局号码一一对应，则采用 DDI 方式。而对于一般的小企业，推荐采用非 DDI 方式，降低费用。

- DDI 方式：

  在 DDI 方式下，一般将用户长号的后若干位作为其短号，但 0 开头的号码不能作为内部短号首位，一般在短号前统一增加一位号码作为短号。对于小型企业，一般采用 5 位短号，选择长号的后 5 位，并在前统一加一位数字构建成为用户短号。短号之间可直拨，拨打本地外线需加拨“0”，拨打长途外线需加拨“#”。外部用户拨打 DDI 方式下的用户时，直拨用户长号即可。

- 非 DDI 方式：

  非 DDI 方式下，内部互通仍然为短号直拨方式。出局呼叫时，与 DDI 方式类似，需加拨一个外线字冠“0”即可。为提高外线利用效率，出局的号码由 AR 智能选

择一个空闲的出局号码出局，也即每次呼叫时出局号码可能不同。非 DDI 方式下，外线入局必须先拨总机号码，按照语音提示转拨分机号码，或拨话务员接入号码后，由话务台转接。

8.3.4 路由设计

- IP PBX 的局内路由：

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

- IP PBX 的出局路由：

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

8.3.5 语音业务设计

IP PBX 还可以提供丰富的语音业务应用，充分满足客户的使用需求。比如：

- 支持号码显示类业务，如：主叫号码显示、主叫号码限制、号码变换等。
- 支持呼叫保持类业务，如：呼叫转移、呼叫保持、呼叫等待、呼叫前转、三方通话等。
- 支持呼叫控制类业务，如：呼叫权限控制、免打扰、呼叫拒绝、呼叫拦截等。
- 支持群组类业务，如：同振、顺振、同组代答、指定代答、一机多号等。

8.3.6 语音可靠性设计

大型企业总部可以部署两台主备 IP PBX，双机备份。总部的 IP 话机正常情况下注册在主用 IP PBX 上（分支 IP PBX 中继到总部主用 IP PBX 上）。当主用 IP PBX 出现故障，IP 话机切换注册到备用 IP PBX 上，切换后可以正常语音通话。

分支 AR 设备作为 IP PBX，在 WAN 中断时，本分支内呼叫可以本地存活，支持断电逃生，同时可以通过 PSTN 或者 IMS 网络出口逃生。

8.3.7 语音 QoS 设计

- IP 话机 QoS：

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

- POST 话机 QoS：

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

- PC 软终端 QoS：

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

- 网络设备的 QoS：

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

8.4 中小型机构高级语音方案特点

中型机构分布式多分支语音解决方案特点：

- 可通过 IP 网络承载，节省企业的长途通信费用。
- SoftoCo 提供丰富的 UC 功能，满足话务前台等功能。
- AR 在分支机构部署，支持本地 PBX，在外网故障情况下，保证本地通话质量。

小型机构分布式多分支语音解决方案特点：

- AR 作为出口路由器，并且兼顾 IP PBX 功能。
- AR 提供企业总机服务，提升企业形象，巩固已有客户资源。
- AR 作为企业语音网关，为分支机构提供 3G 备份，本地存活，提升业务可靠性。
- AR 提供一号通方案，及时寻呼转接，“不错过一单业务”。

9 中小企业典型应用

9.1 经济性酒店解决方案

现代化的酒店都需要一个先进的、可与酒店同步发展的、功能丰富的、易于使用的、可靠的通讯系统和信息管理系统。通过这样的一个信息系统，一方面来为酒店的客人提供及时、准确、可靠、保密的话音、数据、因特网接入等多元化、高质量的酒店通信服务产品；另一方面，通过将酒店本身的管理流程和先进的通信信息系统进行很好的整合，还可以有效地提升酒店的管理效率和管理质量，提升面向酒店客人的整体酒店服务品质。因此，作为经济型酒店信息系统基础的经济型酒店网络系统，在进行整体规划和设计的时候，必须从以下几个方面充分考虑：

- 舒适性

  在网络技术高速发展的今天，网络不仅仅是酒店传播信息的工具，也是保证顾客入住率的有效手段。舒适、随时随地可连接的无线网络，使无线体验更加自由。丰富的语音服务，让顾客住在酒店里更觉方便。

- 高效经济性

  以最小的成本，追求最大利益化的指导原则，要求网络设计经济适用。伴随技术的进步，传统的 TDM 网络、CATV 网络、传统模拟网络逐步 IP 化，大大降低网络成本。基于 IP 统一平台为语音通讯和数字传输提供高速的信息通道，拉近了酒店入住客人、内部办公人员之间以及与外界的距离，实现了建筑内部之间和国内外互通信息，资源共享。

- 绿色节能

  在当前节能、低碳经济的大背景下，酒店行业寄予在信息化和网络技术上的期望值越来越高。不但希望借助信息化的力量，让酒店为顾客提供创新型的服务，提升员工协作效率及客户满意度，更希望能有效控制运营所带来的能源消耗，从而在缩减运营成本、提高收益的同时，打造一个绿色节能的个性化酒店。

- 安全性

  酒店网络中有酒店的大量商务机密数据，客人在使用网络时需要保证个人信息数据的私密性，在互联网病毒、木马、黑客盛行的时代，网络的安全同时也影响到酒店网络的稳定性，酒店网络的安全性对网络管理人员来说是项极大的挑战。

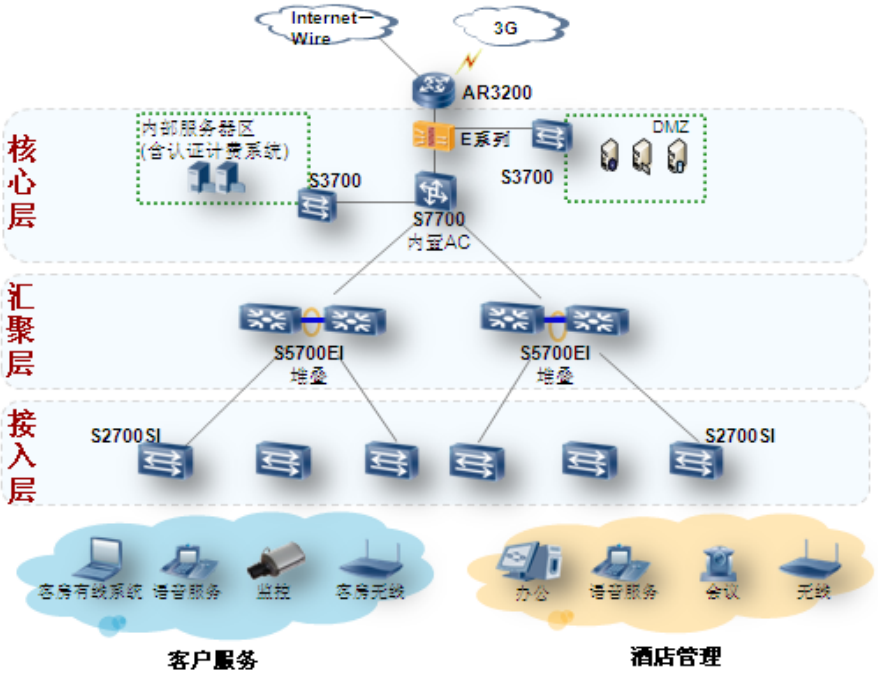
  除了物理设备上的安全性以外，还包括数据通信安全、网络的运行安全。网络安全重在管理，严格的管理是保证网络安全高效运行的重要环节。

- 连锁品牌

在我国酒店行业中，欠缺的不是经济型酒店的产品形态，而是群体意义上的经济型酒店品牌。酒店品牌是酒店产品与产品之外被顾客接收的一切总和。如何使各个连锁酒店分店，能够准确表达相同的品牌理念，服务质量，保障酒店客户、会员对品牌的忠诚度？关键在于连锁酒店的标准化管理体制。通过酒店统一营销平台，总部同经济酒店分店远程互联互通远程监控管理，大大提升酒店管理能力，提升统一的酒店品牌形象。

华为总结多年的建网经验，以实用为原则，通过标准化产品，将语音、视频、数据统一承载，利用互联网和多媒体技术将沟通无限延展。方案通过简易可靠基础网络方案保障其网络可靠性和可扩展性，通过安全、可靠的分支远程管理方案保障分支企业品牌理念一致性问题；通过酒店部署无线，语音等方案使酒店业务更加丰富；通过系列化绿色环保设计，打造绿色“ONE NET”网络。

图9-1 经济型酒店物理架构



9.2 经济型酒店网络规划

9.2.1 核心层设计规划

在酒店典型的层次化模式中，组件间通过核心层互联，核心层用作网络骨干。核心层只作为三层交换环境，通过路由互通实现三层网络的互通。内部服务区直接连接在核心交换机上。建议采用 S7700 系列交换机汇聚内部服务器区、DMZ 区和接入区流量，使内部服务器区、DMZ 区、Internet 区和内部业务区进行互联，支撑内外部的业务流量。核心层部署专业防火墙设备，实现安全防护的同时也作为单点远程用户接入 VPN 的网关，实现单点用户与总部酒店内部的互访。

9.2.2 汇聚层设计规划

汇聚层汇聚来自接入层的节点，保护核心层免受来自接入层高密度设备的影响。汇聚层通常以三层交换机的形式部署，针对网络核心层连接使用三层交换，对接入层连接使用二层交换服务。负载平衡、服务质量(QoS)等都是汇聚层的主要考虑因素。

汇聚层的高可用性通过两条等成本路径来提供，包括从汇聚层到核心层以及从接入层到汇聚层的链路，可在链路或节点发生故障时提供确定性的快速收敛。当冗余路径存在时，故障切换主要依赖硬件链路故障检测，而不是基于定时器的软件故障检测。

汇聚层用于汇聚楼层用户间的流量，同时提供到核心层的流量。采用 S5700 堆叠设备作为汇聚交换机，不但能将保证接入层与核心层之间的互访，同时，在可靠性上也可通过堆叠技术充分保证。

9.2.3 接入层设计规划

接入层为用户提供各种接入方式，是终端、边缘和 IP 电话等设备接入网络的第一层，一般都部署二层设备，有线智能系统通过 S2700 交换机接入、无线用户通过 WA600 系列 AP 进行无线接入。

9.2.4 出口设计规划

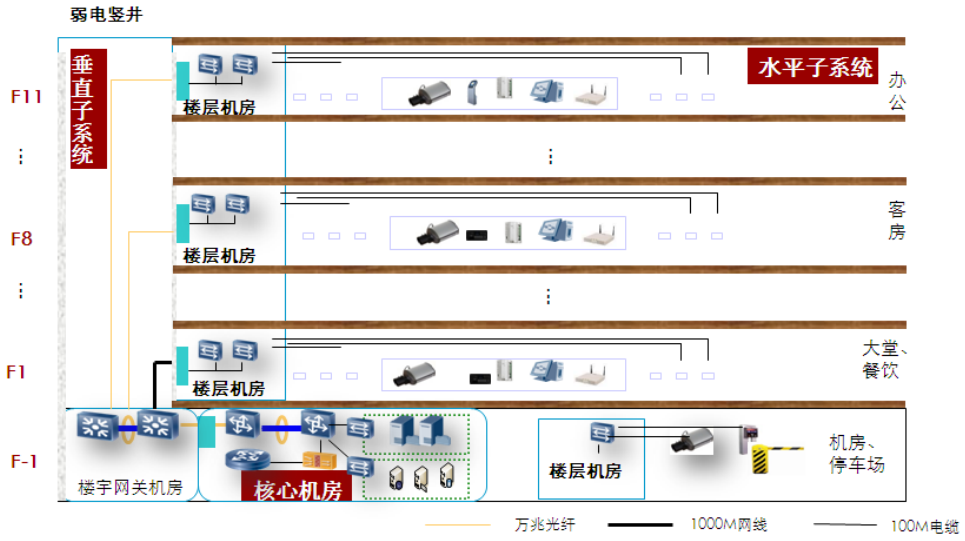
酒店解决方案推荐采用 AR3200 系列接入路由器做酒店的出口路由器。华为第三代 AR 路由器支持防火墙、IPSec VPN 集成，同时提供硬件 QoS 技术，在保证业务质量同时，对转发性能影响通过 HQoS 提供语音、视频、数据的统一承载。随着 3G 业务的不断推广，使用 3G 作为一种链路备份的手段是更加经济实惠的选择，可以替代原先常用的双线备份模式。

9.2.5 可靠性设计规划

酒店上行出口采用 WAN 和 3G 链路备份方式，以 WAN 侧链路为主用链路，3G 链路平时不使用，仅作为备份。S5700 交换机采用堆叠技术，将多台 S5700 交换机虚拟化为 1 台设备，一旦主用 S5700 交换机出现故障后，其他交换机能立即接替其成为主用交换机。

9.3 经济型酒店网络方案

9.3.1 经济型酒店的网络部署



通常核心机房，统一监控多栋楼宇状态，数据统一集中管理；垂直子系统，连接楼宇机房和楼层机房，同弱电系统统一部署；楼宇网关机房主要由汇聚交换机和部分分布式子业务设备组成，将独栋大楼核心业务进行汇聚；水平子系统，以楼层机房为中心，采用接入交换机将各个业务单元接入。

不同酒店建设规模、建筑楼层结构，在方案中有部分差异，主要是选择的设备差异、带宽差异大、组网方案差异大、网络结构差异大、布线差异大、投资差异大，下面简单地探讨一些基本规律。

一般情况下，建议楼层比较多的酒店采用三层结构：核心层，汇聚层和接入层。核心层位于酒店的中心机房，汇聚层在楼层较多的时候可以汇聚到楼层配线间，接入层也分布于各楼层配线间。楼层比较少的酒店，建议采用二层结构，核心层和接入层，核心层位于酒店的中心机房，接入层位于各楼层配线间。

网络核心采用 S7700 系列设备，S7700 可以集成 AC 用来管理 AP 设备。通过千兆多模光纤链路连接汇聚层交换机，汇聚层交换机建议使用 S5700 系列设备，通过堆叠实现汇聚层交换机的备份，提高可靠性。接入层交换机推荐使用 S2700 PoE 交换机，支持在线供电，为无线 AP 和 IP 电话提供持续供电。

- 接入层设备推荐：
  - 对于无线区域选择 PoE 交换机，对于无线 AP 提供远程供电。
  - 在经济型酒店可以考虑 S2700 进行接入，具有较好的控制管理能力。华为拥有丰富款型的百兆接入交换机供选择。采用百兆接入交换机，可以参考低层楼宇部分的选型考虑。
  - 为了满足技术先进性，后期业务扩展性，在办公区接入层可以采用了千兆接入交换机（S57 系列）。S5700-EI/S5700-SI 都是性价比很高的千兆二层交换机。上行链路可以采用万兆光纤，这样可以使每个接入用户可以获得足够高的带宽。也可以先使用多个千兆捆绑方式上行，以后需要时采用万兆链路。

- 核心层/汇聚层设备推荐：
  - 核心设备故障会影响到整个酒店的网络使用，因此必须具备足够高的可靠性和稳定性，此外还必须具备很强的扩展性、多业务支持能力、安全防护能力、大容量接入能力等。
  - S5700/S7700 等高端交换机，是国内外主流的核心交换机之一，拥有数十项可靠性技术保障，并且在国内网上有大量的应用，成熟稳定性已经经历了充分考验。
  - 为了实现大楼不同部门网络之间的安全隔离，以及防范来自外网对大楼内部网的各种网络安全威胁，需要核心交换机支持集成各种安全业务板卡，以方便地实现安全防范技术的部署。S7700 交换机可支持防火墙等多种业务板卡，实现高集成度低成本的安全部署。
  - S77 集成无线 AC 能力，能够较好的适合 Fit AP 的布放，进行整网无线 AP 统一管理控制。

9.3.2 经济型酒店无线网络部署方案

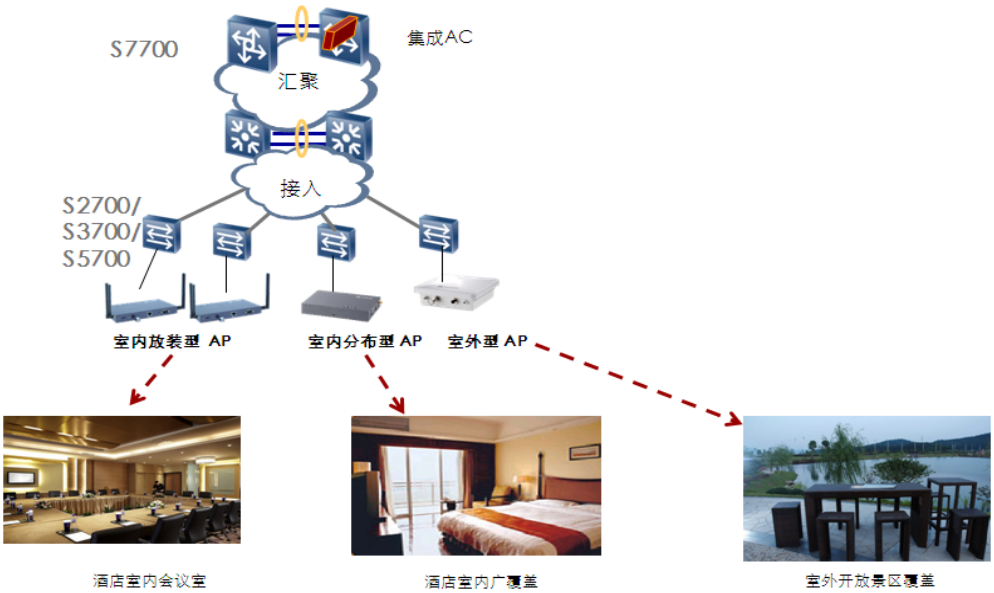
网络需求

传统的 Internet 的固定接入已经不能满足大型酒店日常管理办公和顾客休闲娱乐的需求，迫切需要发挥 WLAN 可移动性的优势，为各个酒店提供更多的增值服务。

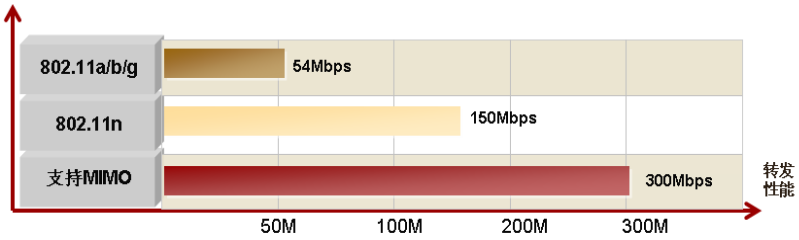
WLAN 的部署需要根据不同的目标区域提供不同的 WLAN 覆盖方案，根据覆盖区域和用户要求的不同，可以采用室内直接覆盖、室内分布式覆盖、室外覆盖室内、室外覆盖等多种覆盖方案。

解决方案

酒店网络建设主要考虑大堂和会议室、住宿房间等人员相对集中、数据业务量需求较高的热点区域。大型会议室和住宿房间对容量有较高要求，对其网络建设以容量为主；展厅和包间对容量有要求一般，网络建设时覆盖为主，同时考虑容量需求。

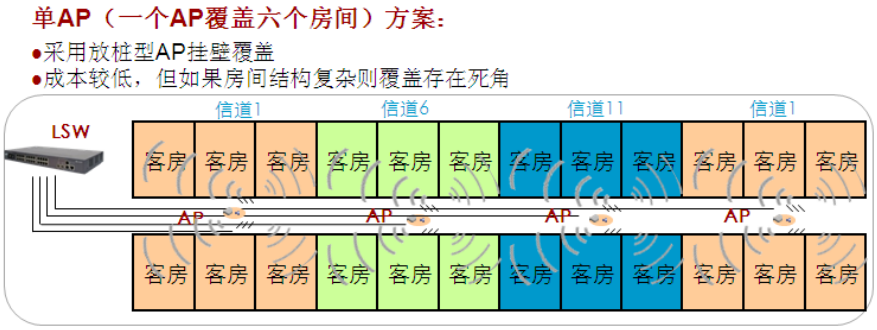


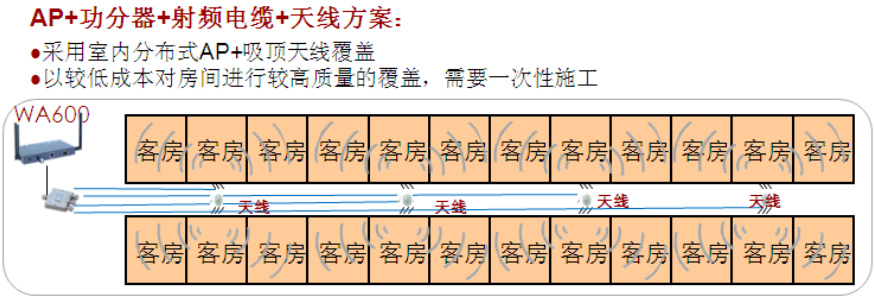
室内直接覆盖方案适用于用户密度高、信号衰减小的区域，如大堂、会议室等区域；室内分布式覆盖方案适用于用户密度不高，信号衰减大的区域，如 KTV 包间、住宿包间等区域。



伴随无线技术的发展，802.11n 技术可以将 WLAN 的传输速率由目前 802.11a 及 802.11g 提供的 54Mbps，提高到 300Mbps 甚至高达 600Mbps。得益于将 MIMO（多入多出）与 OFDM（正交频分复用）技术相结合而应用的 MIMO OFDM 技术，提高了无线传输质量，也使传输速率得到极大提升。

在覆盖范围方面，802.11n 采用智能天线技术，通过多组独立天线组成的天线阵列，可以动态调整波束，保证让 WLAN 用户接收到稳定的信号，并可以减少其它信号的干扰。因此其覆盖范围可以扩大到好几平方公里，使 WLAN 移动性极大提高。





华为针对客房无线覆盖，提供两套方案：

- 方案一：采用单 AP 方案，能够较好覆盖客房死角，不需要一次性投资。
- 方案二：AP+功分器+射频电缆+天线，以较低的成本进行酒店覆盖，但是需要一次性施工完成。

根据不同经济酒店建筑结构特点，可以进行选择。针对酒店的各种标准间或豪华套间，对无线信号的屏蔽高、人员集中、拥有电脑数量较多（平均每 5 个旅客拥有一台笔记本

电脑）的情况，拟采用全向吸顶天线，采用在满足边缘场强的基础上采用多天线，小功率的覆盖方式，保证天线覆盖区域一定的重叠；天线安置于相邻两个包间门口的走廊天花板上方，减小无线信号的穿墙损耗；针对标间数量较多、顾客拥有电脑数量较多，加上用户接入数量的限制，方案二中每层采用一个 AP、单主干覆盖设计，其 AP 固定在每层走廊西侧安全出口旁的弱电间内，通过 PoE 供电，PoE 供电模块安放在设备箱内；交换机安装在每层的弱电间内，确保交换机到各楼层 AP 间的网线长度不超过 90 米。

9.3.3 经济型酒店安全部署方案

网络需求

经济型酒店网络的安全建设，集中体现在以下五个方面：

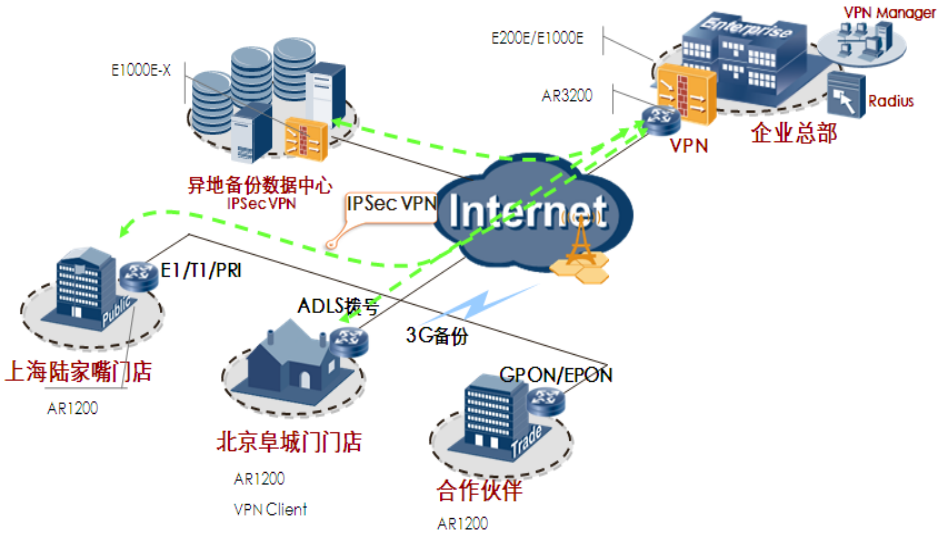
- 连锁酒店分支安全连接。
- 在 Internet 出口，对病毒、垃圾邮件和网络攻击进行过滤和防御。
- 确保内部网络安全，防止来自内部攻击。
- 酒店 Web 页面推送。
- 管理酒店客户上网行为，符合国家 82 号令明令要求各企业不得发布非法言论的要求。

对此华为推出了一个能与基础网络深度融合，能将多种安全防护手段有机结合的协同、立体安全防护新一代产品与解决方案。

解决方案

- 远程接入方案

  连锁酒店互联，在 VPN 方式下，VPN 客户端和设置在内部网络边界的 VPN 网关使用隧道协议，利用 Internet 或公用网络建立一条“隧道”作为传输通道，同时 VPN 连接采用身份认证和数据加密等技术避免数据在传输过程中受到侦听和篡改，从而保证数据的完整性、机密性和合法性。通过 VPN 方式，酒店可以利用现有的网络资源实现远程用户和酒店门店机构对内部网络资源的访问，不但节省了大量的资金，而且具有很高的安全性。



方案特点：

- 基础一体化

  企业总部可采用 AR3200 系列提供防火墙、IPSec VPN 集成方案，通过 HQoS 提供语音、视频、数据的统一承载。

- 3G 备份

  随着 3G 业务的不断推广，使用 3G 作为一种链路备份的手段是更加经济实惠的选择，可以替代原先常用的双线备份模式。

- 边界安全—防火墙部署

  重点关注酒店出口，对物理分区间、业务分区间进行隔离或进行访问控制，保证分区的安全。推荐在核心交换机与 Internet 路由器之间配置防火墙。可根据规模和安全性要求，对出口路由器、防火墙、核心交换机采用冗余设计，保证系统的可靠性。

  方案特点：

  - 配置防火墙全面安全防范能力，通过防火墙的访问控制策略，控制来自 Internet 的用户只能访问 DMZ 区服务器的特定端口，对内部用户访问 Internet 进行基于 IP 地址的控制。安全区域划分阻止安全威胁扩散。
  - 网络、应用、数据立体的防御体系能够应对多样的安全威胁。
  - 防火墙同核心交换机防护功能结合，提供低成本、不同层次网络安全隔离。

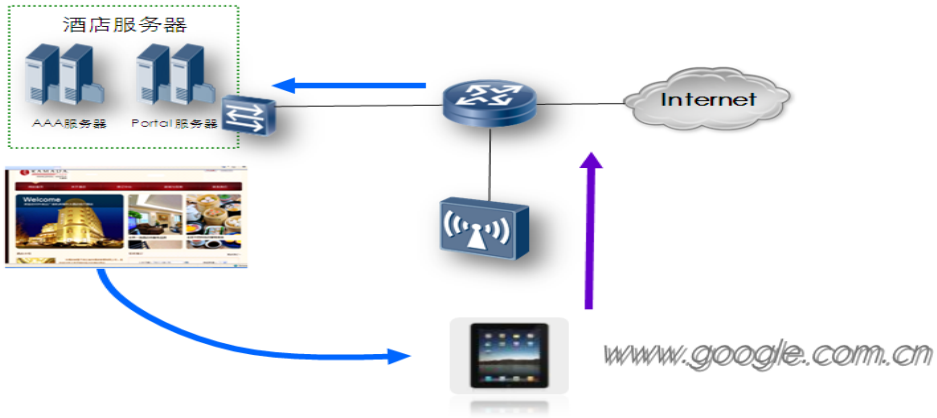
- 内网防护

  对于内网威胁，可以考虑在核心层、汇聚层、接入层分别部署不同特性。如：在接入层部署 MFF 功能，防止用户非法互访。通过在接入层配置 MAC 限速，防止 MAC 泛洪；在汇聚层配置 IP Souce Gurad 来防止 IP 欺骗，也可以考虑配置 DHCP 限速防止 DHCP 泛洪；在网关部署 ARP 严格学习或部署 ARP 防 IP 攻击功能来阻止 ARP 仿冒网关攻击、配置 APR 源抑制功能来防止 APR 泛洪攻击，这部分功能也可以部署在防火墙上，在接入层部署 DHCP Snooping 功能丢弃非法入侵的 ARP 报文。

- 酒店 Internet 出口访问重定向方案

  让客人在酒店访问 Internet 时顺道访问酒店的主页是一个很对客户营销酒店品牌和理念的好办法。酒店客户上网时，Web 页面重定向到一个 portal 页面，在 portal 页面上有酒店的广告、宣传等信息和相关的链接，可以达到宣传酒店的目的。用户再

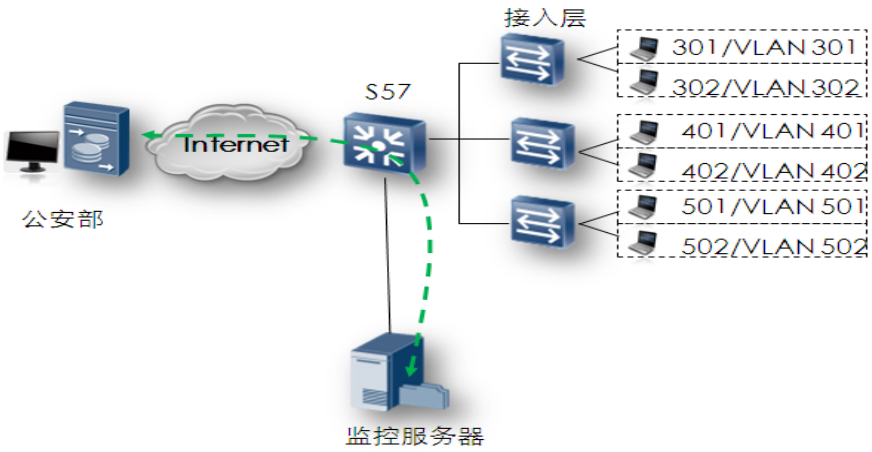
次访问网络，可以直接访问 Internet，这样既可以达到宣传酒店的作用，同样满足可以上网需求。



- 酒店客户上网信息安全管理

  根据公安部 82 号令　第五条“公安机关公共信息网络安全监察部门负责对互联网安全保护技术措施的落实情况依法实施监督管理”，北京出台《关于开展非经营性上网服务场所依法落实安全技术保护措施的通知》规定，自 2011 年 6 月起，“宾馆、酒店、图书馆电子阅览室、歌厅、洗浴、学校电教室等提供上网服务的场所”，都要“全面落实安全技术保护措施建设”。至于如何落实安全技术保护措施，公安部门要求商家购买并安装“互联网公共上网服务场所安全管理系统”。

  推荐采用为每个房间划分一个 VLAN，通过对应的 VLAN ID 来识别房间号，完成用户上网行为的记录、跟踪、分析、日志记录，实现各种条件下的查询功能。



  在管理服务器上安装公安系统提供的监控软件，利用交换机提供的端口镜像功能，通过 VLAN ID 号监控每个房间的上网信息并实时发到公安部门，轻松实现监控。

- 带宽流控方案

  酒店用户上网高峰期时，在接入交换机上为每个房间分配一个 VID，在接入层部署 VLAN，在汇聚层为用户分配 VLAN，并对用户进行流量峰值控制。在出口路由器部署 QoS，将语音业务、办公数据、每个客房用户分配队列，实现 QoS 调度。

方案优势：

根据客户上网时数，平均分配上网带宽，保障客户实时享受最大平均上网带宽。

9.3.4 经济型酒店 IP 语音通信方案

网络需求

经济型连锁酒店，一般客房 50～300 客房，以 200 客房的经济型酒店为实例，典型的用户规模在 250 人左右，但考虑到举办商务会议、新闻发布会等活动时候可能峰值人数会增加至 500 人左右。

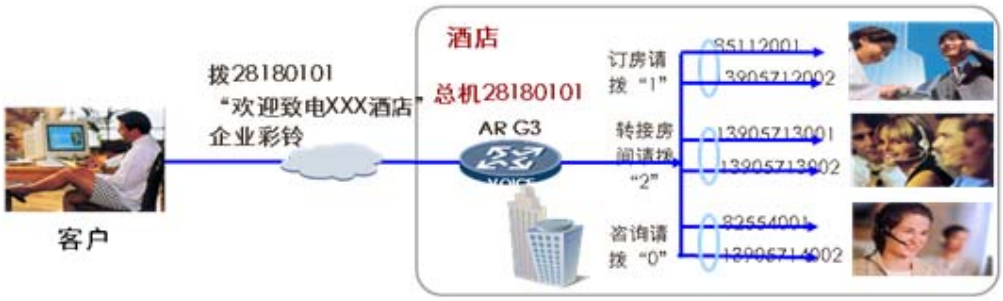
为了提高酒店的服务水平，争取更高的星级评价和提供增值服务功能，基础网络同时考虑将语音、视频、数据统一承载，保障无线业务安全性，语音业务 QoS。

经济型酒店对 IP 语音提供丰富业务、低资费感兴趣，经济实惠的电话网络解决方案已经成为许多经济型酒店的迫切需求。与普通电话相比，IP 电话的优势是非常明显的，因为 IP 电话将电话网络整合到数据网络中，省去了庞大的 PSTN 长途话费开支，可以显著降低企业网络的运营成本。

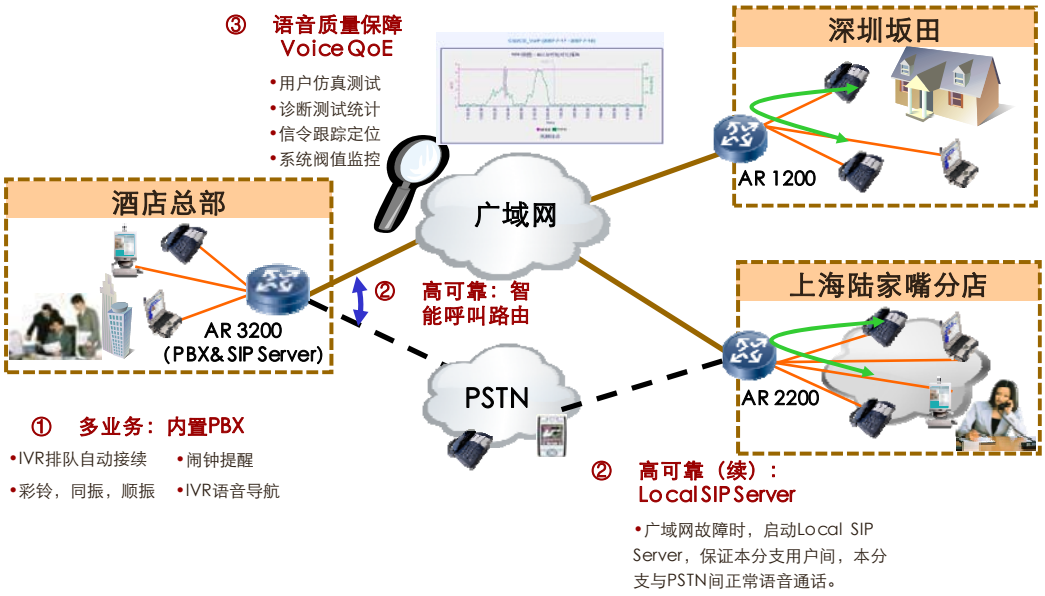
华为语音解决方案包含一系列智能、简便、安全和综合化的产品、服务，专为中小型企业设计，能够帮助企业控制成本、对竞争压力做出迅速反应并提升经营效率。这一行业领先的解决方案能够统一企业中所有通信及商业过程，为企业增加强势支持和完全可管理的 IP 语音及数据网络服务，使企业能够专注于企业的核心竞争力，增强经营能力，壮大企业发展。

中小型宾馆对语音通讯方面主要有如下需求：降低通讯费用，便于计费统计，方便日常维护。

外部客户拨打酒店电话，根据企业提示彩铃拨打分机号，AR G3 自动总机功能能够直接识别分机号对应的号码，进行转接。



解决方案



酒店总部以及各个分支的出口语音设备分别部署 IP PBX。总部采用 SoftCo 设备充当 IP PBX，可以提供丰富的补充业务；分支采用 AR 设备，既充当出口路由器，又充当分支 IP PBX 功能。各分支和总部的语音用户在本地完成用户注册和呼叫控制，总部 IP PBX 为各个分支互通提供呼叫路由，形成总部为一级呼叫路由，分支为二级呼叫路由的结构。IP PBX 设备下挂 IAD 设备，一方面扩大了接入用户数量，另外一方面提供了 POTS 话机的接入方式，实现模拟信号到数字信号的转换。总部和分支 IP PBX 设备分别接入当地运营商网络，可以是 IMS 或者 PSTN。企业可以为分散在不同城市的办公分支提供 VoIP 服务，不同分支间可使用企业短号进行通话。企业对分支所在地的外线呼叫可通过 IP 网络承载，节省企业的长途通信费用。

方案特点：

- 华为语音平台共享，业务快速发布
- 与 MSAN、MxU 统一语音平台
- 支持 VoIP/MoIP/FoIP；
- 支持 H.248 及 SIP 协议；
- 支持丰富的 PBX 功能；
- 支持 G.711/G.729/G.723 编解码；
- 支持抖动缓冲/回声消除/丢包补偿

9.4 经济型酒店网络方案特点

- 简易网络，业务隔离、受限互通

  采用简易一体化方案。大大降低网络建设和管理成本，节省出口链路租赁成本。

专业业务 VLAN 隔离，在接入和汇聚后，通过核心交换机互联。

- 可靠性高

  汇聚采用堆叠＋端口捆绑的树形网络，网络既简单又可靠，还能保证链路带宽的负载均衡使用。

- 有线无线一体化

  在 S77 上集成无线 AC 控制器，结合最新 802.11n 技术。有效地将有线网络和无线网络统一结合，简化网络配置，提供大带宽网络。

- 网络安全

  全网所有终端采用 Portal，在接入设备上实施 IP＋MAC 绑定，用户间隔离并防 IP 地址盗用。

  OA 网中的用户均认证后接入、对用户进行安全检查和权限控制。

  在各业务子网（含服务器机房）的汇聚交换机上部署防火墙或通过 ACL 实施相互隔离。

- 绿色环保

  通过系列化绿色环保网络设备，打造绿色“ONE NET”网络。

10 设备说明

10.1 S9300 系列

Quidway®S9300 系列运营级园区核心交换机是由华为公司自主开发的新一代高性能核心路由交换机产品，提供大容量、高密度、模块化的二到四层线速转发性能，具有强大组播功能，完善的 QoS 保障、有效的安全管理机制和电信级的高可靠设计，满足高端用户对多业务、高可靠、大容量、模块化的需求，降低运营商的建网成本和维护成本，可广泛应用于构建各种类型的园区网核心层。对于汇聚交换机性能和接口密度要求高的某些大型园区网，也可使用 S9300 系列交换机作为汇聚交换机使用。

表10-1 S9300 系列交换机

产品型号	说明
S9303	支持 3 块 LPU 交换网容量 720Gbit/s 背板容量 3Tbit/s 转发能力 540Mpps
S9306	支持 6 块 LPU 交换网容量 2Tbit/s 背板容量 6Tbit/s 转发能力 1080Mpps
S9312	支持 12 块 LPU 交换网容量 2Tbit/s 背板容量 12Tbit/s 转发能力 1320Mpps

图10-1 S9303 外观图

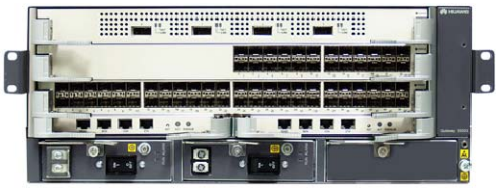


图10-2 S9306 外观图

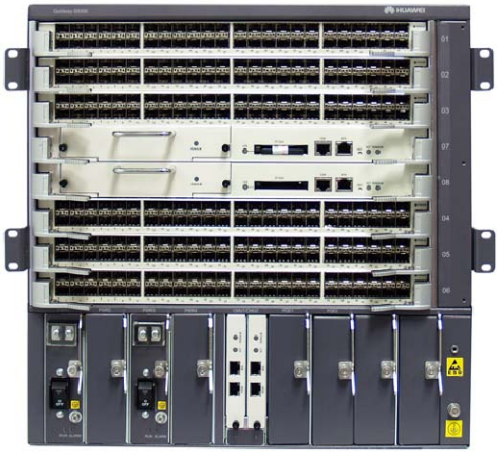
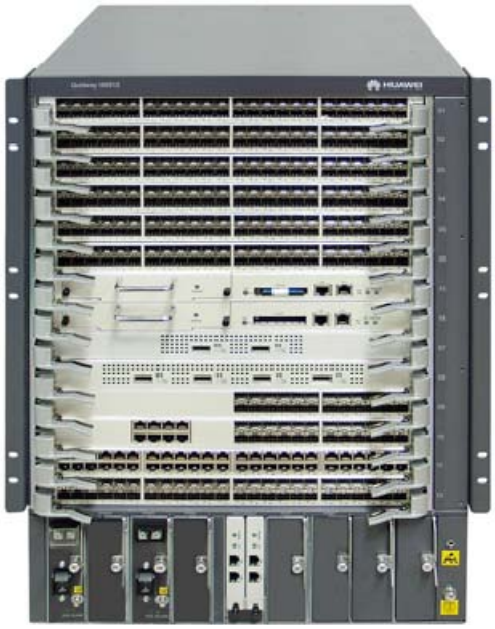


图10-3 S9312 外观图



S9300 系列交换机具体以下特点：

- 先进体系结构，高性能，配置灵活
  - S9300 系列交换机采用先进的全分布式体系结构设计，采用业界最新的硬件转发引擎技术，所有端口支持的业务能够线速转发，业务包括 IPv4/MPLS/二层转发等。支持 ACL 线速转发。
  - S9300 系列交换机实现组播线速转发，硬件完成两级复制：交换网板复制到接口板和转发引擎复制到接口。
  - S9300 支持 2Tbps 交换容量，支持多种高密度板卡，满足核心、汇聚层设备大容量、高端口密度的要求，可以满足用户日益增长的带宽需求，能够极大的保护和节约用户投资。
- 完善的安全机制
  - S9300 系列交换机支持 OSPF、RIP v2 及 BGP v4 报文的明文及 MD5 密文认证，支持安全的 SSH 登录、命令行分级保护、基于用户安全策略的 SNMP V3、DHCP Snooping、IP Source Guard、DAI（Dynamic ARP Inspection）、层次化 CPU 通道保护，并提供以下几种用户认证方式：本地认证、RADIUS 和 HWTACACS 认证。
  - 支持防网络风暴攻击、防 DOS/DDOS 攻击、防扫描窥探攻击、防畸形报文攻击、防网络协议报文攻击等安全技术。
- 全面的可靠性
  - S9300 系列交换机最大支持 128 个汇聚组，每个汇聚组内支持最多 8 个成员端口，支持跨单板端口间的汇聚。
  - 支持 DLDP（Device Link Detection Protocol）：可以监控光纤或铜质双绞线的链路状态。如果发现单向链路存在，DLDP 会根据用户配置，自动关闭或通知用户手工关闭相关端口，以防止网络问题的发生。
  - 支持 RRPP 及多实例。相比其他以太环网技术，RRPP 具有以下优势：拓扑收敛速度快，低于 50ms。收敛时间与环网上节点数无关，可应用于网络直径较大的网络。
  - 支持标准 STP/RSTP/MSTP 二层环网保护协议。
  - 支持 SmartLink 及多实例。
  - 支持 BFD for 单播路由/VRRP/FRR/PIM。

10.2 S7700 系列

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

表10-2 S7700 系列交换机

产品型号	说明
S7703	支持 3 块 LPU 交换网容量 288Gbit/s 背板容量 1.2Tbit/s 转发能力 215Mpps
S7706	支持 6 块 LPU 交换网容量 1.536Tbit/s 背板容量 2.4Tbit/s 转发能力 432Mpps
S7712	支持 12 块 LPU 交换网容量 1.536Tbit/s 背板容量 4.8Tbit/s 转发能力 864Mpps

图10-4 S7703 外观图

图10-5 S7706 外观图

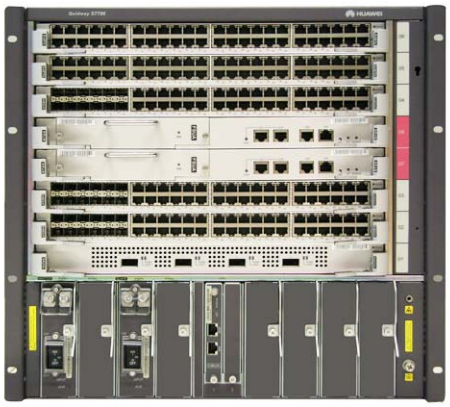
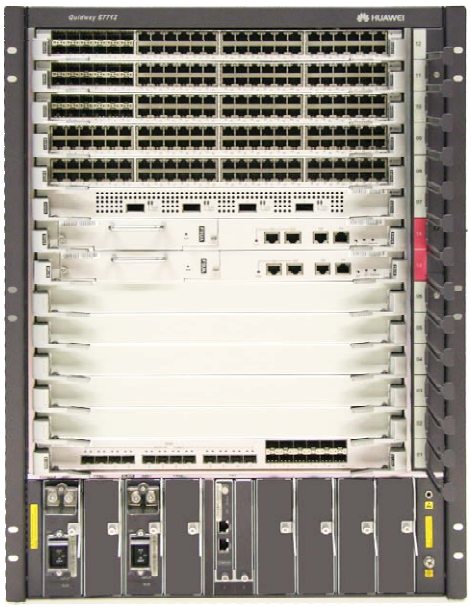


图10-6 S7712 外观图



S7700 系列产品有如下特点：

- 先进体系结构，高性能，配置灵活
  - S7700 系列交换机采用先进的全分布式体系结构设计，采用业界最新的硬件转发引擎技术，所有端口支持的业务能够线速转发，业务包括 IPv4/MPLS/二层转发等。支持 ACL 线速转发。
  - S7700 系列交换机实现组播线速转发，硬件完成两级复制：交换网板复制到接口板和转发引擎复制到接口。
  - S7700 支持 1.536Tbps 交换容量，支持多种高密度板卡，满足核心、汇聚层设备大容量、高端口密度的要求，可以满足用户日益增长的带宽需求，能够极大的保护和节约用户投资。
- 完善的安全机制
  - S7700 系列交换机支持 OSPF、RIP v2 及 BGP v4 报文的明文及 MD5 密文认证，支持安全的 SSH 登录、命令行分级保护、基于用户安全策略的 SNMP V3、DHCP Snooping、IP Source Guard、DAI、层次化 CPU 通道保护，并提供以下几种用户认证方式：本地认证、RADIUS 和 HWTACACS 认证。
  - 支持防网络风暴攻击、防 DOS/DDOS 攻击、防扫描窥探攻击、防畸形报文攻击、防网络协议报文攻击等安全技术。
- 全面的可靠性
  - S7700 系列交换机最大支持 128 个汇聚组，每个汇聚组内支持最多 8 个成员端口，支持跨单板端口间的汇聚。
  - 支持 DLDP，可以监控光纤或铜质双绞线的链路状态。如果发现单向链路存在，DLDP 会根据用户配置，自动关闭或通知用户手工关闭相关端口，以防止网络问题的发生。

- 支持 RRPP 及多实例，相比其他以太环网技术，RRPP 具有以下优势：拓扑收敛速度快，低于 50ms。收敛时间与环网上节点数无关，可应用于网络直径较大的网络。
- 支持标准 STP/RSTP/MSTP 二层环网保护协议。
- 支持 SmartLink 及多实例。
- 支持 BFD for 单播路由/VRRP/FRR/PIM。

10.3 S5700 系列

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

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

表10-3 S5700 系列交换机

产品型号	设备外观图	备注
S5700-28C-EI		三层交换机 • 下行 24 个 GE 电 • 上行支持三种插卡 1、4 个 XGE 光 2、2 个 XGE 光 3、4 个 GE 光 • 增强三层功能
S5700-28C-EI-24S		三层交换机 • 下行 24 个 GE 光 • 上行支持两种插卡 1、4 个 XGE 光 2、2 个 XGE 光 3、4 个 GE 光 • 增强三层功能

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

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

S5700 系列交换机的特点是：

- 电信级的可维护性
  - S5700 遵循电信级标准设计，风扇、电源可现场更换，方便维护；机箱重量轻，可以安装在 600mm 深机柜中，且安装方便。
  - S5700 提供软件热补丁技术，实现设备软件在线平滑升级。
  - S5700 支持快速保护倒换机制 RRPP（Rapid Ring Protection Protocol），可以快速实现链路级和业务级保护倒换，满足运营级的可靠性要求。
- 强大的多业务接入能力
  - S5700 通常部署在企业网的汇聚层，可直接接入来自下游 AMG（Access Media Gateway）和 LSW（LAN Switch）等设备的业务，并汇聚到上游设备。可接入的业务包括：VoIP、IPTV/VOD（Video On Demand）视频业务以及宽带上网业务。

- S5700 采用成熟、经济的 IP 内核技术，借助高性能 ASIC（Application Specific Integrated Circuit）芯片，提供大容量的数据交换能力，满足传统电信业务对低时延抖动、高可靠性的需求。S5700 采用以太网组网技术，支持组播业务，提供良好的 QoS 机制和多种保护倒换技术，实现了良好的带宽保证和多业务支持能力。

- 灵活的组网能力
  - S5700 提供 10/100/1000BASE-T 以太网电接口、100/1000BASE-X 以太网光接口及万兆以太网光接口，支持 Access、Trunk 和 Hybrid 等多种接口类型。
  - 对于千兆光纤连接，S5700 提供可插拔的 SFP（Small Form-Factor Pluggable）类型光模块。对于万兆光纤连接，S-switch 提供可插拔的 XFP（10Gigabit SmallForm Factor Pluggable）和 SFP+（SmallForm-Factor Pluggable Plus）类型光模块。光纤长度可以根据用户对传输距离的需求灵活选配。
  - S5700 可以组成树状、星型和环状以太网。对于环状以太网，S5700 提供 STP（Spanning Tree Protocol）和 RRPP，消除环路并提供快速保护倒换。
- 网络级 QoS 保障

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

  S5700 保障设备和数据传输的安全，有效的防止恶意用户对网络的攻击。
  - 支持基于 MAC 地址的过滤。
  - 提供丰富的 ACL 策略。
  - 提供“VLAN＋MAC”的查表机制。
  - 支持流量抑制。

  S5700 提供安全的用户登录操作保护。
  - 对登录用户提供口令保护，口令可加密功能。
  - 通过配置用户级别和命令级别实现对命令的分级保护。
  - 通过命令锁定当前配置终端，防止设备被非法使用。
  - 对影响系统性能的重要命令，提供确认和提示。

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

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

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

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

- 绿色节能设计

  S5700 采用多种节能措施，包括：

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

- 先进的防雷技术

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

- 人性化的 PoE 供电方式

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

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

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

10.4 S3700 系列

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

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

表10-4 S3700 系列交换机

产品型号	设备外观	备注
S3700-28TP-SI	AC  DC 	三层交换机 • 下行 24 个 FE 电 • 上行 2 个 GECombo 和 2 个 GE 光 • 基本三层功能

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

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

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

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

10.5 S2700 系列

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

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

表10-5 S2700 系列交换机

产品型号	设备外观	备注
S2700-9TP-EI	AC  DC 	以太网交换机 • 下行 8 个 FE 电 • 上行 1 个 GECombo • 支持 ACL

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

由于采用相同的软件平台，S2700 在很多软件特性上与 S3700 基本一致，最大的不同在于 S2700 为二层交换机，因此不具有三层相关的特性和功能，而 S3700 同时支持二层和

三层的硬件线速转发。在硬件设计上，S2700 大部分型号采用自然散热的无风扇设计，包括 S2700-9TP-PWR-EI、S2700-9TP-SI/EI、S2700-18TP-SI/EI、S2700-26TP-SI/EI 等。

10.6 AR 系列

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

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

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

表10-6 AR 系列产品

产品型号	设备外观	备注
AR1220		整机容量：8Gbps 转发性能：350Kpps/200Mbps(64byte)
AR1220V		整机容量：8Gbps 转发性能：350Kpps/200Mbps(64byte)
AR1220W/1220VW		整机容量：8Gbps 转发性能：350Kpps/200Mbps(64byte)
AR2220		整机容量：32Gbps 转发性能：1Mpps/500Mbps(64byte)
AR2240		整机容量：80Gbps 转发性能：2Mpps/1333Mbps(64byte)
AR3260		整机容量：160Gbps 转发性能：3.5Mpps（SRU80 高性能主控板）/2000Mbps(64byte)

AR 系列产品的特点如下：

- 高性能

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

- 多业务集成

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

- 强大的 QoS

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

- 高密度接入

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

- 丰富的广域网接口

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

10.7 防火墙系列

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

表10-7 防火墙系列产品

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

产品型号	设备外观	备注
E1000E-U5		• 固定接口：4GE 电+4GECombo • 支持万兆接口 • 标配双电源(AC/DC 可选) • 扩展槽：2*FIC • 吞吐量：10Gbps
E1000E-U6		• 固定接口：4GE 电+4GECombo+8GE 光 • 支持万兆接口 • 标配双电源(AC/DC 可选) • 扩展槽：2*MIC+5*FIC • 吞吐量：20Gbps

防火墙系列产品的特点是：

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

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

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

    关键部件冗余配置，成熟的链路转换机制，支持光、电两类内置 Bypass 插卡，为您提供超长无故障硬件保障；商用 10 年以上的超稳定软件平台，全球在线设备超过 10 万台，为您打造永续的办公环境。
- 超千种应用程序的精细管理，创建更高效的网络
  - 广泛应用识别，实现网络可视化：150 名应用识别专家，超过 850 种可识别应用分类，让您一目了然网络带宽应用。
  - 海量网站分类，营造绿色上网环境：6500 万海量网站，超过 130 种内容分类，屏蔽挂马、钓鱼等恶意网站，防范员工不当操作危害内网安全；隔离赌博色情等不良网站，营造绿色上网环境。
  - 精细应用管理，创建高效办公网络：基于时间、应用、用户、带宽、连接数的多方位调控手段，可有效保障关键业务带宽，提升带宽利用率和员工工作效率，让 P2P/IM/Web 网站随您掌控。
- 专业内容安全防御技术的重新演绎，提供更安全的网络
  - 业界领先反病毒引擎，提供 99%高精准检出率：基于 Symantec 多年积累的反病毒技术，采用文件级内容扫描的 AV 引擎，结合全球领先的仿真环境虚拟执行技术，提供高达 99%的精准检出率，多次荣膺国际评测组织好评。

- 专业漏洞补丁技术，让“变形”无所遁形：传统基于攻击代码的防护方式，因为攻击种类的频繁变形，需要维护更新庞大签名库，使得 IPS 引擎不堪重负，检测性能低下，误报漏报率较高。E1000E-X 采用 Symantec 领先的漏洞防护技术，针对漏洞（而非攻击代码）提供“虚拟补丁”，让各种攻击变形无所遁形。
- 专业团队实时更新，实现零日攻击防护：全球部署的蜜网系统和超过 300 人的专业安全分析团队，持续追踪最新、最热门、最高危的系统漏洞和软件漏洞，以最快速的应对方案实现零日攻击防护，为您提供更安全的办公网络。

- 一键式配置，让策略调优化繁为简
  - 图形化配置界面，从此告别命令行：基于 Web 界面配置管理，更直观、更简单，彻底摆脱繁琐的配置。
  - 专业配置向导，轻松搞定策略配置：每项独立业务，均提供专业配置向导，让管理员轻松搞定策略配置。
  - 一键开启 IPS 和 AV，减轻维护工作量：基于 99%高精准检出率的 IPS/AV 规则库，无需调测，直接开启，将管理员从费时、费力、繁复的策略调优中彻底解放出来，真正实现快速部署，即插即用。