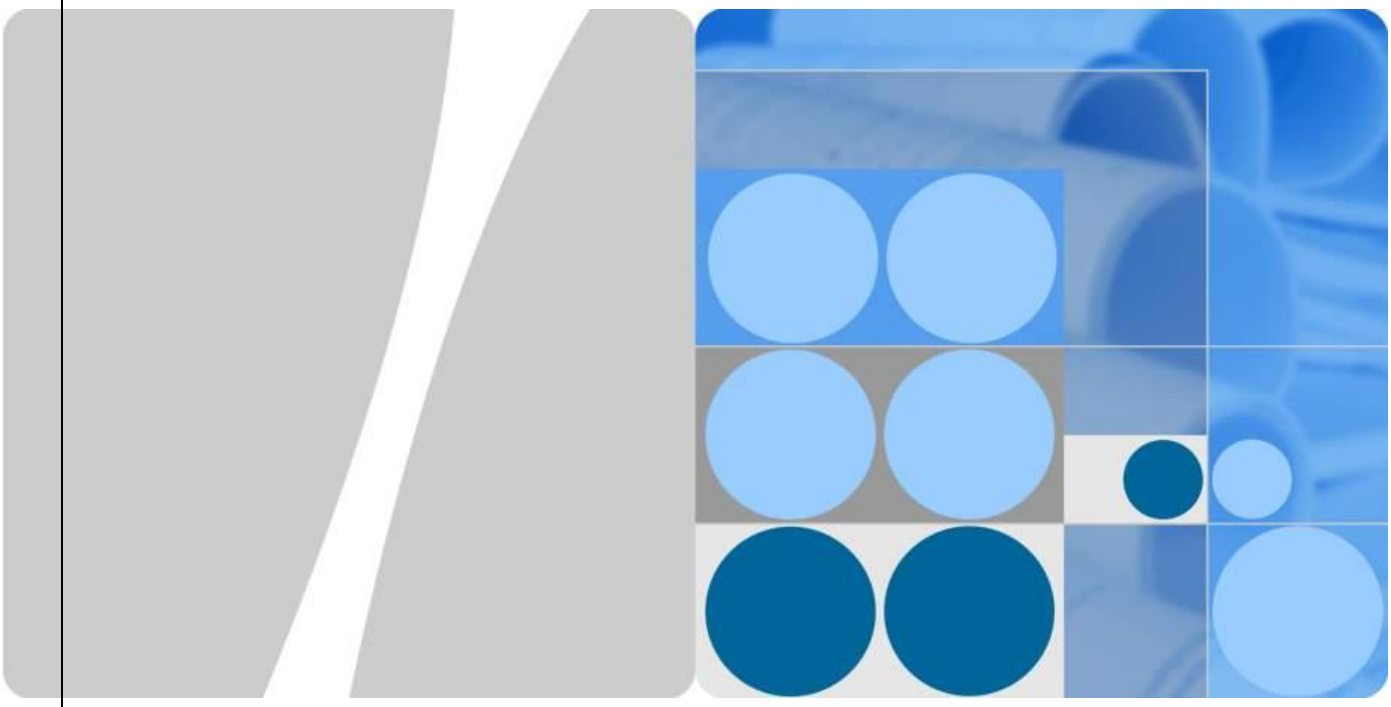
资料编码



华为 AAA(认证授权计费)解决方案
销售一指禅

华为技术有限公司

华为 AAA（认证授权计费）解决方案销售一指禅

1 华为 AAA（认证授权计费）解决方案简介

本方案介绍了企业网络 AAA 管理方案，应用于酒店和校园等具有运营需求的网络应用场景，包括有线和无线一体化认证计费方案，根据不同的应用场景，共有四套差异化 AAA 方案。

华为 AAA 解决方案以“安全、灵活、便捷”为特点，向用户提供安全控制、接入认证、控制授权、计费策略、流量控制和报表功能，共计六大功能，并支持按照不同行业使用场景差异化部署：

- **接入认证：**支持 MAC 认证、802.1x 认证、Portal 认证、PPPoE 认证等多种认证方式，根据场景灵活选用；
- **控制授权：**包括用户组、多出口管理、自助注册功能；
- **计费策略：**按月/流量/时长、支持预付费后付费、支持上网时段限制、支持购卡自助冲值；
- **流量控制：**支持用户带宽限制、IP 组限速、支持实时流量统计；
- **安全控制：**防代理技术、用户强制下线、系统支持多机热备、系统支持负载均衡；
- **报表功能：**TOPN 报表、IP 当前流量报表、用户统计报表、财务分析报表。

2 华为 AAA（认证授权计费）解决方案产品列表

AAA 方案产品如表 1，根据不同 AAA 方案，计费网关可以选择：

- BRAS 设备 ME60
- Srun 3000
- Dr.COM 2166

AAA 服务器系统可选择以下合作方产品：：

- 深澜软件：AAA 服务器选择深澜软件 Srun 系统；
- 城市热点软件：AAA 服务器选择城市热点 Dr.COM 系统。

	产品/型号
接入交换机	S5700、S3700、S2700、S1700

	产品/型号
汇聚交换机	S7700、S5700
核心交换机	S9700、S7700
WLAN AC	S9700 AC 插卡、S7700 AC 插卡、AC6605
WLAN AP	AP6010、AP6310、AP6510、AP6610、AP5010、AP7110
AAA 服务器	深澜软件 Srun 服务器系统
	城市热点 Dr.COM 服务器系统
客户端	深澜软件 Srun 客户端
	城市热点 Dr.COM 客户端
计费网关	深澜软件 Srun 3000
	城市热点 Dr.COM 2166
	BRAS 设备 ME60

表 1　AAA 解决方案产品列表

3 园区网 AAA（认证授权计费）解决方案核心卖点

- 用户认证

认证方案中，用户准入认证可选择 MAC、802.1X、Portal 认证方式，用户准出认证一般采用 Portal、PPPoE 认证（如表 2 所示）。

认证方法	认证点	技术特点	应用场景
MAC 认证	准入	① 无需客户端，IP 地址认证后分配； ② MAC 地址存在仿冒风险，安全性较低。	① 园区准入认证场景，哑终端采用 MAC 准入认证； ② 准入认证点在接入层或者汇聚层交换机上。
802.1X 认证	准入	① 需要客户端，IP 地址认证后分配； ② 二层认证方式，安全性较高。	① 园区准入认证场景，用户采用 802.1X 准入认证； ② 准入认证点在接入层或者汇聚层交换机上。

Portal 认证	准入准出	① 无需客户端，IP 地址认证前分配； ② 三层认证方式，控制点在网关，安全性较高。	① 适用于园区准入或者准出场景，准入认证点在汇聚或者核心交换机上； ② 准出认证点在园区出口计费网关上。
PPPoE 认证	准出	① 需要客户端，IP 地址认证后分配； ② 需要 BAS 设备配合，认证报文封装开销大，安全性较高。	① 适用于园区准出认证场景，用户采用 PPPoE 认证。 ② 准出认证点在园区出口计费网关上，计费网关一般为 BRAS 设备，如 ME60。

表 2 认证方式对比

- 用户授权

用户授权是指用户认证通过后，基于用户角色来对网络访问权限进行的策略控制。通过授权策略，在准入认证阶段，可防止用户非法接入园区内网和非授权访问其他机密资源；在准出认证阶段，可控制用户访问外网的带宽，限制访问非法网页和网站等 Internet 资源。

用户授权方案有三种类型：动态 VLAN、动态 ACL 和用户组授权，对于无线用户，一般在 AC 集中认证，授权下发到 AP 设备。

- 动态 VLAN 授权方式部署简单，维护成本也较低，但相对而言，其控制粒度在 VLAN 层面，适用于在同一办公室或同一部门所有人员权限相同的场景。
- 动态 ACL 授权方式能做到最大程度的权限控制，可以分别对每个用户权限精细控制，适用于同一部门内员工具有不同访问权限的场景，比如部门经理比普通员工具有更大的权限。
- 用户组是指具有相同角色、相同权限等属性的一组用户（终端）的集合。例如，园区网中可以根据企业部门结构划分研发组、财务组、市场组、访客组等部门用户组，对于不同部门可授予不同安全策略。

- 计费策略

园区网 AAA 方案采用城市热点或者深澜软件的服务器平台，提供灵活多样的计费管理：

- 支持按流量、时间和包月计费；支持按期限、合约方式计费；
- 支持临时、专线储值卡方式计费；
- 支持按国内、国外流量分开计费；
- 支持按不同目标地址（DAA）及服务计费；
- 支持充值卡充值、网上自助服务；
- 可以实现以上多种计费策略灵活组合计费；
- 支持设定时间上限、流量上限、最低消费、信用额度、费用封顶等多项控制参数。

计费方案采用城市热点（国内转售）或者深澜公司（国内推荐销售）的专业计费平台，实现针对不同场景计费，有如下 4 套差异性解决方案（如表 3）：

	计费方案	方案特点	应用场景	推荐产品
1	计费网关一次认证方案	① 计费网关做准出认证，不部署准入认证； ② 准出采用 Portal 认证，内网互访不限制； ③ 计费网关一次认证，方便管理维护。	适用于中、小型规模园区，如酒店等运营网络，特别是对于内网准入没有过多要求的企业。	计费网关和服务器系统推荐合作方产品。
2	准入准出认证分离方案	① 计费网关做准出认证，采用 portal 方式； ② 有线用户准入认证在交换机上，无线用户 AC 集中认证,可以选择 1x/portal ③ 准入准出分离控制，增强内网安全性。	本方案适于大、中型规模园区，如星级酒店、高等院校等，特别是对于内网准入具有安全要求的运营网络。	计费网关和服务器系统推荐合作方产品。
3	IPv4/IPv6 双协议栈方案	① IPv6 计费网关做准出认证，Portal 认证； ② 有线和无线 IPv6 用户均在 IPv6 网关上做准入认证，推荐 Portal 认证方式； ③ 双栈用户一个帐号，提升用户体验。	本方案适于有 IPv6 计费需求的园区，特别是需要部署 IPv4/IPv6 的网络。	计费网关和服务器系统推荐合作方产品。
4	大二层园区网计费方案	① ME60 构建大二层园区网络，准入准出认证点合一,内网 QinQ 隔离； ② 认证方式为 Portal 或者 PPPoE 认证； ③ DAA 机制按目的地址计费，提供创新商业模式。	本方案适用于高等院校等大型园区，选择高性能 BRAS 设备 ME60 做计费网关。	计费网关采用 ME60，服务器系统推荐合作方产品。

表 3 认证计费方案

4 华为 AAA（认证授权计费）解决方案竞争力

方案优势	引导思路
用户管理	基于用户组（user-group）管理用户和授权策略，方便 AAA 部署，节省用户资源。

安全管理	（1）多维度策略管理，可基于用户、时间、部门实施控制；支持基于位置的策略自适应（基于 IP 地址族），实现不同网关区域的差异化控制。 （2）安全策略可通过网站安全中心，用户自己下载策略，支持策略自定义。
补丁管理	支持完整的补丁管理方案，包括补丁下载、验证、分发、统计等功能；支持与 WSUS 联动。
病毒管理	支持强联动，和江民、金山等厂商合作，可主动实施病毒查杀和修复，其他厂商弱联动。
多样性的计费策略	支持按流量计费； 支持按时长收费； 提供包月、包流量等多种计费策略； 通过基于用户的流量限制，支持多个出口分别计费和不同目的地址分别计费等计费管理措施和丰富的计费策略。
华为高性能 BRAS（ME60）计费系统	大容量、高密度的用户管理 ，支持多达 256K 并发用户处理能力。 电信级可靠性 ，ME60 依靠独有的热备份技术，支持 PPPoE 和 DHCP 单板和设备间的热备份，倒换时，用户不用重新拨号，业务永不中断。 DAA 功能 ，按目的地址（目的网段）区分不同的业务类型，实现用户不同业务类型的流量统计；
高性能的认证计费系统	**并发能力：** 单台设备同时可以支持 32000 人在线，每秒支持 1000 人同时认证（ 网关模式下） 单台设备同时可以支持 64000 人在线，每秒支持 1200 人同时认证（ Radius 模式下）

5 华为 AAA（认证授权计费）解决方案典型应用场景

5.1 计费网关一次认证方案

5.1.1 应用场景

对于中、小型规模园区，如酒店等运营网络，一般对于内网准入没有过多要求，只在计费网关做准出认证。

5.1.2 方案部署

计费网关一次认证方案（如图 1），准出认证部署在计费网关上，一般选择 Portal 认证方式，有线、无线用户统一在计费网关上做准出认证，认证通过后开放访问 Internet 权限，开始计费。

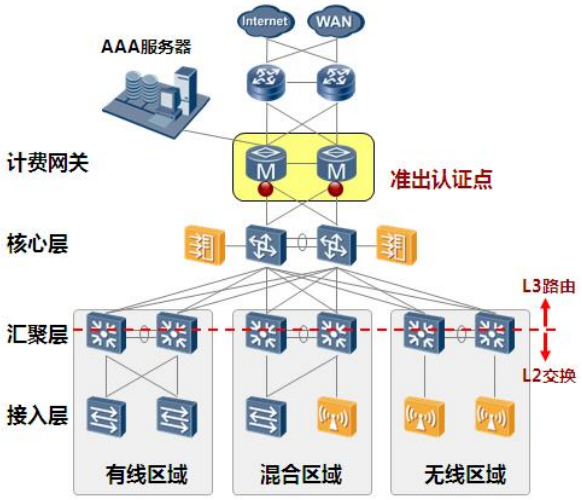


图 1 计费网关一次认证方案

5.2 准入准出认证分离方案

5.2.1 应用场景

本方案适于大、中型规模园区，如星级酒店、高等院校等，特别是对于内网准入具有安全要求的运营网络。

5.2.2 方案部署

计费网关一次认证方案(如图 2)，准入和准出认证分开部署，准入认证可选择 802.1X 或者 Portal 认证；准出认证一般采用 Portal 认证，用户准出认证通过后，开放访问 Internet 权限，并进行计费。

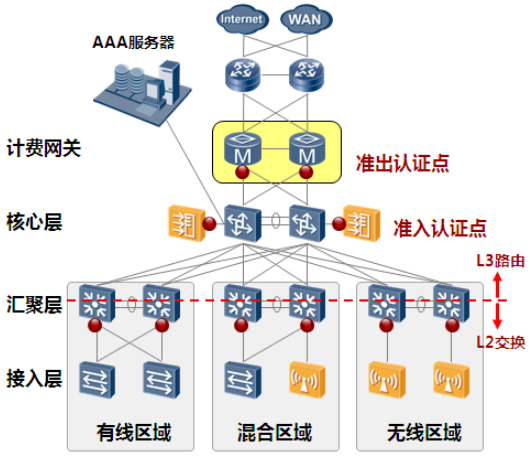


图 2 准入准出认证分离方案

5.3 IPv4/IPv6 双协议栈方案

5.3.1 应用场景

本方案适于有 IPv6 计费需求的园区，特别是教育行业，需部署 IPv4/IPv6 双协议栈网络。

5.3.2 方案部署

对于部署 IPv4/IPv6 双栈方案的园区网（如图 3），IPv6 孤岛和 IPv4 网区和相互隔离，需要在准入准出认证分离方案的基础上，叠加 IPv6 认证计费。

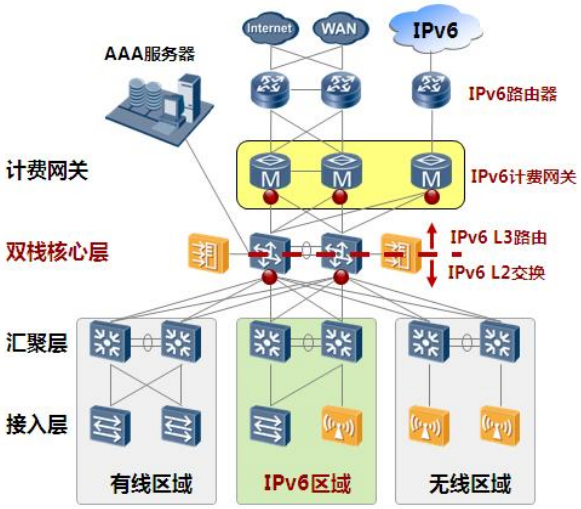


图 3 IPv4/IPv6 双协议栈方案

5.4 大二层园区网计费方案

5.4.1 应用场景

对于规模比较大的园区场景，譬如高等院校想打造高品质园区，选择高性能 BRAS 设备 ME60 做计费网关，可以简化配置和管理，构建大二层园区网。

5.4.2 方案部署

该网络拓扑方案（如图 4），两台 ME60 双机热备，作为整个园区网的认证计费网关，用户准入和准出认证合一，部署在 ME60 上，可选择 Portal 或者 PPPoE 认证方式。

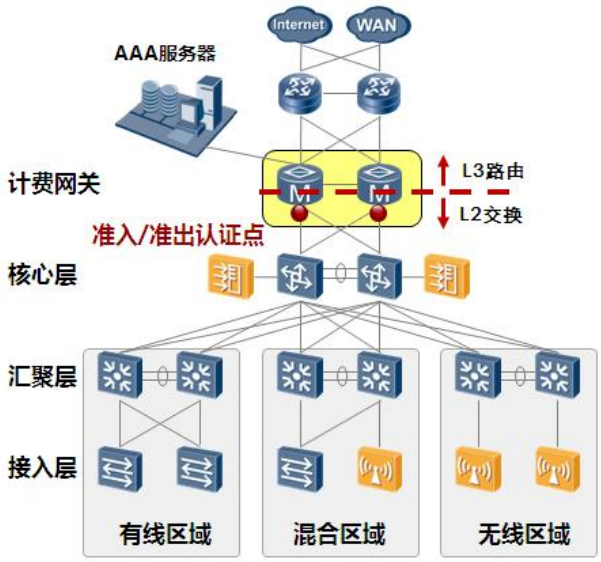


图 4 大二层园区网计费方案