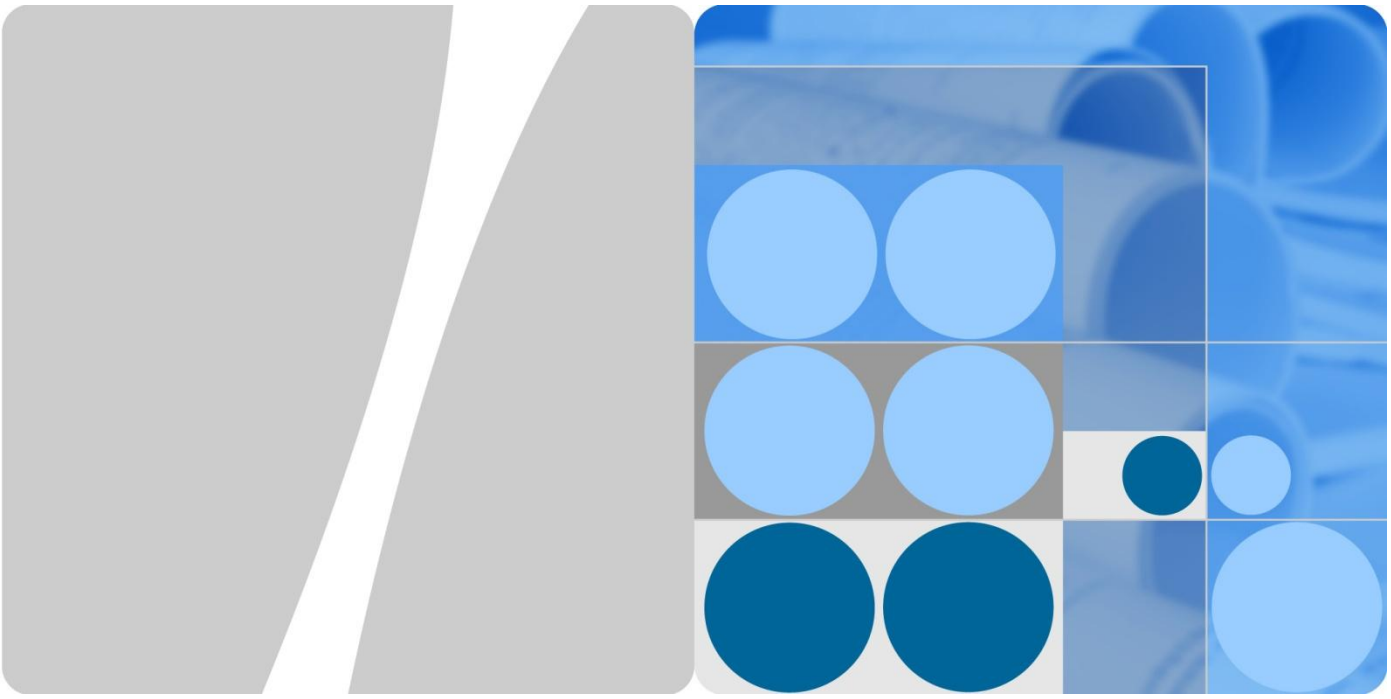


ONE NET Campus 园区网 AAA 解决方案

技术建议书

文档版本 01

发布日期 2012-09-30

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

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

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://enterprise.huawei.com

客户服务邮箱： ChinaEnterprise_TAC@huawei.com

客户服务电话： 400-822-9999

目 录

1 园区网 AAA 方案概述

1.1 方案背景

AAA（Authentication Authorization Accounting），是指网络的认证、授权和计费方案。其中认证是指验证用户的身份与可使用的网络服务；授权是指依据认证结果为用户开放特定的网络服务；计费是指基于用户上网时间或者访问流量，为网络运营者提供费用结算，增加网络拥有者的收益。

随着网络规模不断扩张，有线、无线网络的相互融合，用户终端数量的剧增，网络复杂度也呈几何级数增长，这些给网络的运营增加了困难。想要成功的实现网络运营，必须综合考虑不同运营对象的上网行为差异，来制定合适的认证、授权和计费策略。例如酒店员工，工作时间网络需求多局限于酒店内网，并且接入 internet 也会因为其酒店员工的身份而不会产生计费；而酒店的客户，上网需求往往是通过酒店局域网出口接入 internet，此时就有了计费的需求。

对于校园网用户而言，往往认证计费的策略又不同。例如，不管对于老师或者学生，一般访问内网不进行计费，而访问外网则需要进行收费，但是在网络权限上，会因为其身份的不同存在差异，具有老师身份的用户拥有更高权限，可以访问一些学生用户不能访问的内网资源。

为了保护网络使用者的合法权益，更为了增加网络拥有者收益，对非运营商拥有的园区网提出了网络运营需求。

1.2 园区网 AAA 解决方案

华为的 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、报表功能六大功能，应用于网吧、酒店、校园网、广电等行业运营级网络。

表1-1 园区网 AAA 解决方案功能列表

功能组件	功能描述
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，根据对象和场景灵活选用。
用户授权	包括用户组、多出口管理、支持上网时段限制。
计费策略	按月/流量/时长、支持预付费后付费、基于 DAA 计费。
流量管理	用户带宽限制、支持实时流量统计。
安全控制	防代理技术、用户强制下线。
报表功能	用户统计报表、计费分析报表、用户上网日志等。

2 AAA 基本技术简介

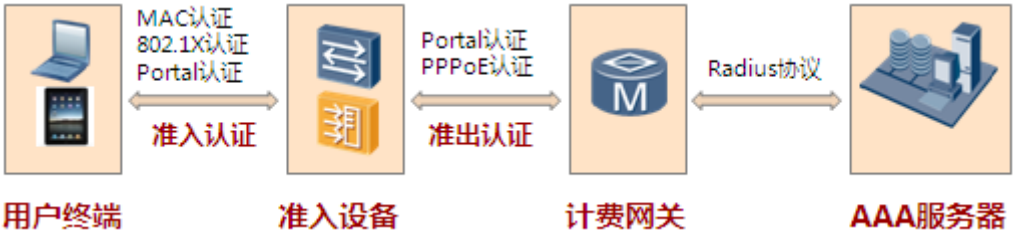
2.1 AAA 系统简介

2.1.1 AAA 系统组成简介

华为的 AAA 解决方案以向客户提供“安全、灵活、便捷”的认证计费方案为主导思想，根据用户使用场景和园区规模，灵活部署合理选用。

如**错误！未找到引用源。**所示，AAA 系统框架中包括四个关键组件：用户终端（客户端）、准入设备、计费网关和 AAA 服务器，其中用户终端包括能够安装代理的 PC、智能终端等设备；AAA 服务器具备认证、授权和计费功能。

图2-1 AAA 系统组成部件示意图



用户终端

用户终端是指接入到网络的 PC、智能手机、平板 PAD 等各种用户终端设备；客户端是安装在用户终端系统上的专用软件，与 AAA 服务器联动进行用户接入认证、用户授权和计费控制等工作。

准入设备

网络准入设备可以是交换机、路由器、AC、AP 等设备，通过这些网络准入设备，实现强制用户内网准入认证、拒绝非法用户的网络访问。

网络准入设备具备如下功能特性：

- 用户准入认证

网络准入设备可协助用户终端完成认证过程，包括 802.1X、Portal 认证、PPPoE 多种认证方式。

- 实现用户策略控制

  网络准入设备可根据准入服务器给出的结果，给用户授予相应内网访问权限。

计费网关

计费网关主要有两个功能：

- 用户准出认证

  作为用户出园区的认证点，控制用户访问外部 Internet 网络，认证方式主要有 Portal、PPPoE 两种方式。

- 用户计费功能

  计费网关可实时统计用户上网流量和上网时间，向 AAA 服务器传送统计信息，完成计费功能。

AAA 服务器

AAA 服务器主要完成用户身份认证、策略下发、上网计费、统计报表等功能。具体参见下一章节。

2.1.2 AAA 服务器介绍

提供多种认证方式

- 提供基于接入层，汇聚层不同的接入方案，适合各种类型园区网使用。
- 提供 802.1x 认证，Portal 认证，MAC 认证，PPPoE 认证等多种认证方式，根据不同使用场景灵活部署。
- 支持多种终端部署，包括 PC 终端、非 PC 终端、无线终端及 IP 电话等。
- 支持有线用户、无线用户统一认证；支持准入、准出分离认证；
- 提供 Agent 客户端，无 Agent 的 ActiveX 插件。

丰富的安全控制

- 支持基于用户、端口或用户组下发 ACL，基于用户和用户组的访问权限控制。
- 能够根据用户终端安全状态进行权限切换。
- 有效识别非法用户，有效防止通过修改 IP 和 MAC 地址私接，保障用户网络安全

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

高可靠性

- 提供 RADIUS 服务器备份及 Portal 服务器备份，可靠性高。
- 计费网关支持单机和主备两种部署方式，主备方式下可以做到用户数据实时同步。用户在任一设备上线后，在线信息会同步到对端设备，保证两台计费网关信息一致，从而提高业务可靠性。
- 提供双机热备、双机冷备、单点逃生等功能。

灵活方便的执行界面

- 提供功能完备，简单易用的操作界面。

便捷的账务管理

- 通过支持购卡充值和自助查询服务，支持多业务合帐等功能，方便企业账务管理的同时也给用户带来便利。

丰富灵活、融合开放的解决方案

- 实现了集中统一的认证、授权管理。
- 充分利用已有的网络安全建设，将各个孤立的解决方案实现最佳的融合。
- 灵活丰富的安全检查，包含了业界最多的终端安全检查策略，并且在用户访问的整个过程当中都可以进行检查。
- 业界一流的高安全性，在系统管理方面，采用基于管理角色的操作权限控制，并记录管理员的操作日志保证提高操作安全性和可追溯性。
- 优异的高可靠性，重要组件均提供主备和负载均衡，提供独有的逃生通道功能。
- 支持 Windows 系统的软件安装，并提供认证配合 Windows 域联合进行认证。

2.2 认证技术介绍

2.2.1 认证协议简介

常用的认证协议有 802.1X、MAC 认证、Portal 认证、PPPoE 认证，其中准入认证包括 MAC、802.1X、Portal 等方式，准出认证包括 Portal、PPPoE 等方式。

2.2.2 MAC 认证

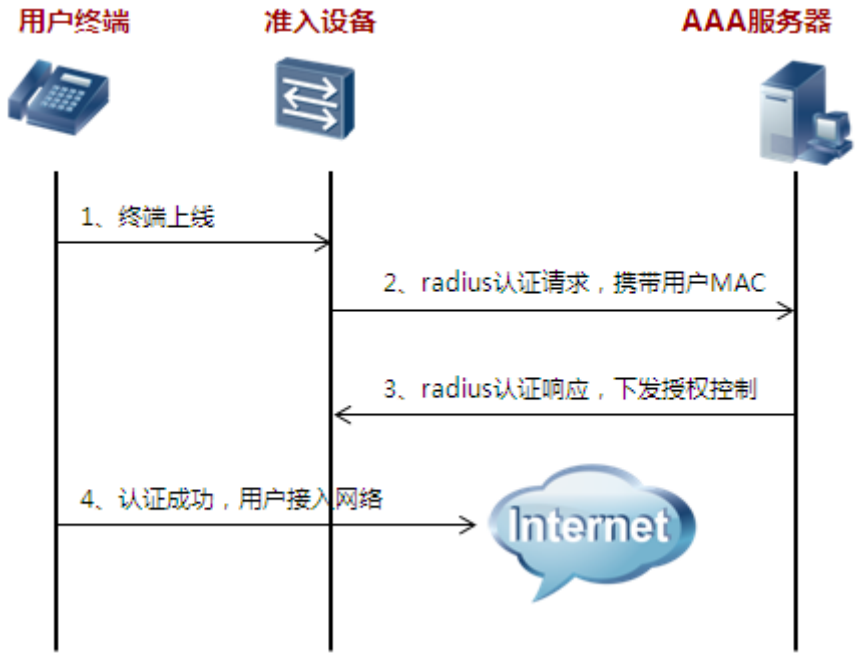
MAC 认证就是以终端的 MAC 地址作为身份凭据到系统进行认证。启用 MAC 认证后，当终端接入网络时，网络准入设备提取终端 MAC 地址，并将该 MAC 地址作为用户名和密码进行认证。如果认证失败使用户下线，并保持一段时间内不再发起认证和探测，超时后重新开始探测过程。如果认证成功，交换机将增加该 MAC 地址进入 MAC 表，用户将可以正常访问网络。

一般对于哑终端，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，此时采用 MAC 认证的方式实现对终端的网络访问控制。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，此时也可采用 MAC 认证方式完成准入认证。

对于用户的 MAC 认证，既可以是本地认证，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。

图2-2 MAC 认证流程图



MAC 认证的详细流程如下：

1. 终端设备上线，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，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。
3. 服务器认证成功，Radius 下发 ACL 或 VLAN 对终端设备进行权限控制；
4. 认证成功，用户接入网络。

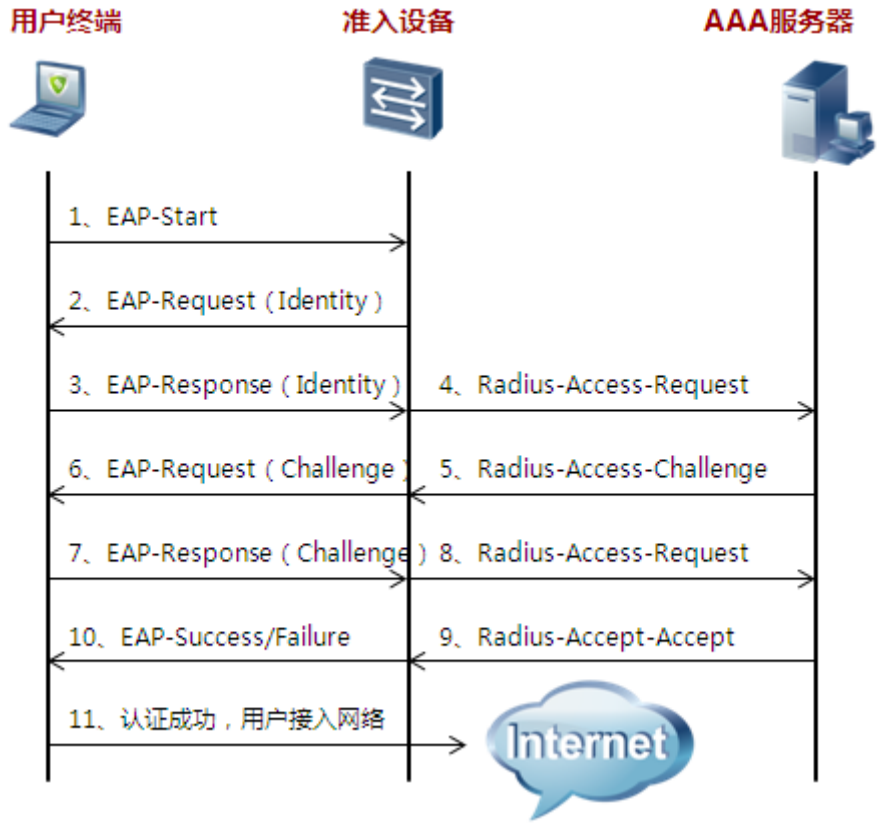
2.2.3 802.1X 认证

802.1X 是一种链路层认证框架，包括客户端、准入设备和认证服务器三部分。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 协议起源于 WLAN 的 802.11 协议，用于控制无线用户的链路层接入和身份认证。经过扩展后，802.1X 也可以使用以太网帧作为承载报文，从而可适用于以太网以及其他的有线接入方式。

802.1X 认证使用 EAP（Extensible Authentication Protocol）认证协议，目前常用认证类型有 EAP-MD5、EAP-PEAP、EAP-TLS、EAP-TTLS 等，不同认证类型，802.1X 认证流程差异较大，下面以 EAP-MD5 为例，简要说明一下协议流程。

图2-3 802.1X EAP-MD5 认证流程图



简要的流程说明如下：

1. 图中 1-4 是用户名上送步骤，用户在客户端输入用户名和密码，其中用户名上送认证服务器处理。
2. 流程 5～6 实现生成 Challenge 挑战字，认证服务器收到用户名后，若数据库存在改用户名，则生成挑战字 Challenge，并通知客户端。
3. 流程 7～8 实现用户密码上送，客户端使用 MD5 算法，使用 Challenge 对密码加密，并上送服务器
4. 通过流程 9～11 实现认证成功授权，服务器收到用户密码（MD5）后，进行验证，符合要求后开发用户权限，用户接入网络。

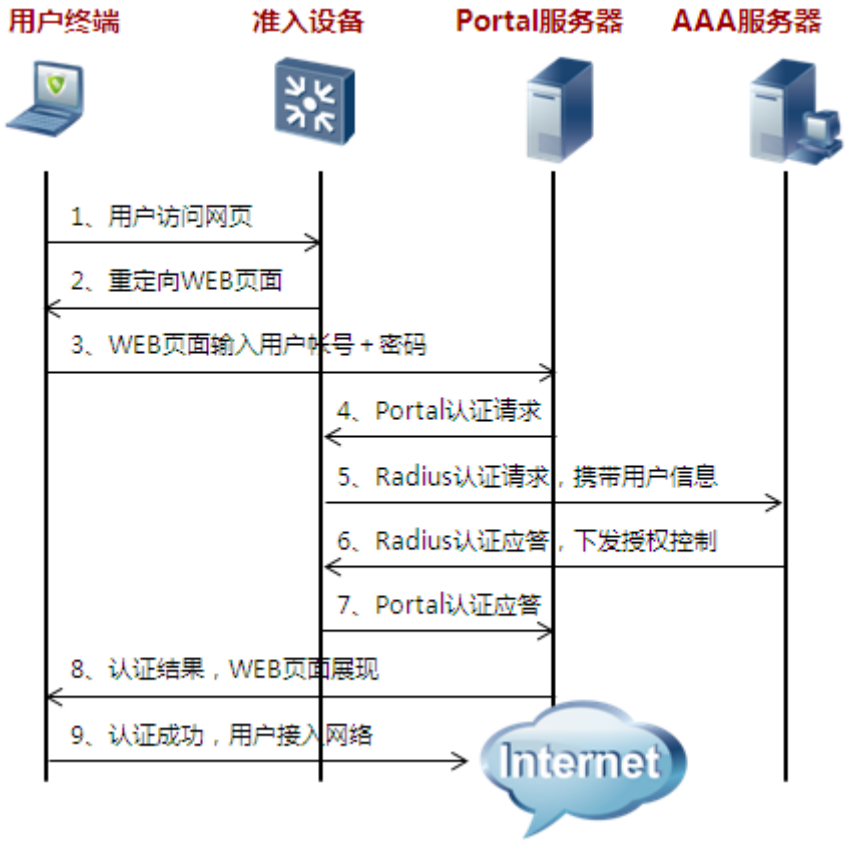
2.2.4 Portal 认证

Portal 认证也称为 WEB 认证或 DHCP+WEB 认证。Portal 认证是一种三层认证方式，客户端使用标准 Web 页面或者客户端，填入用户名、密码信息，提交后由 Portal 服务器、AAA 服务器和网络设备配合完成用户的认证。

Portal 认证可以无需安装客户端软件，这使得 Portal 认证在园区网 AAA 方案中获得广泛的应用。

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。

图2-4 Portal 认证流程图



详细的流程说明如下：

1. 用户终端访问任意 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，向认证服务器（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，一并下发授权控制。
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，用户成功接入网络。

2.2.5 PPPoE 认证

PPP 协议是一种点到点的链路层协议，它提供了点到点的封装、传递数据的方法；如果 PPP 应用在以太网上，必须使用 PPPoE 再进行一次封装，进行广播链路上点对点通讯的

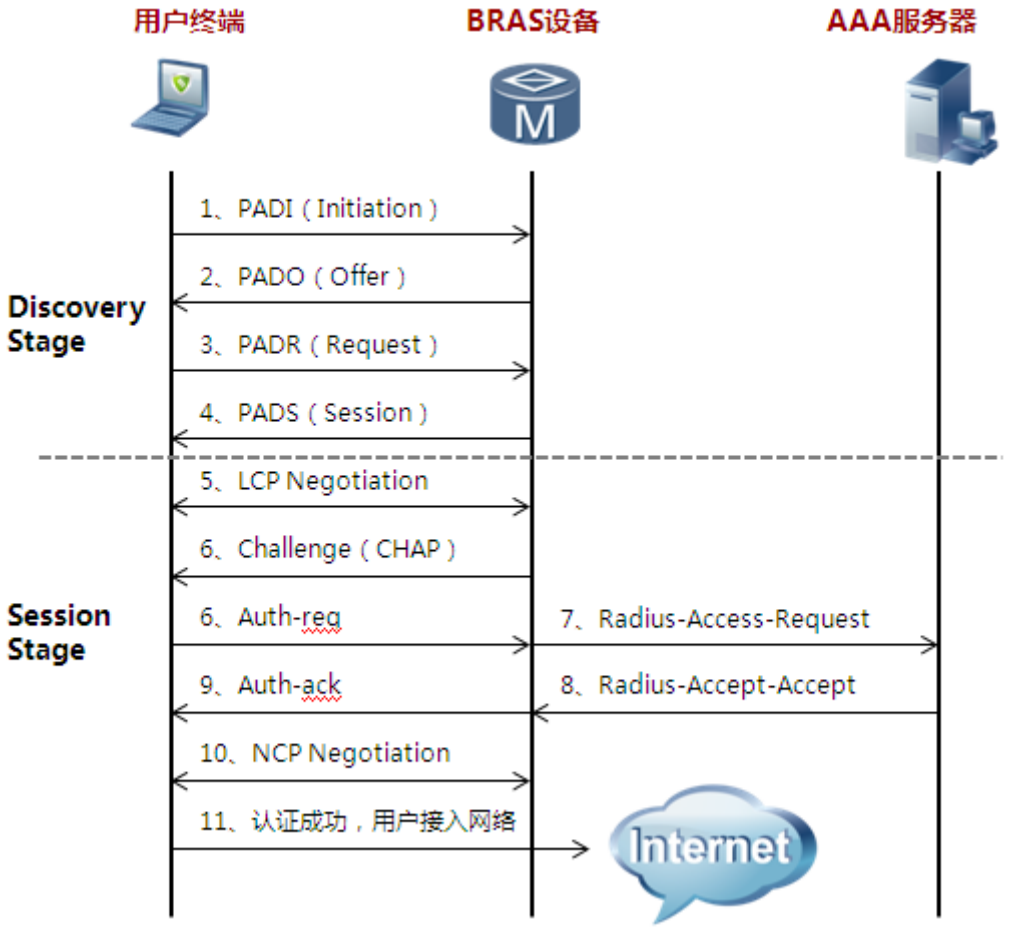
协商，包括服务器的发现和会话标识 Session ID 的确认； PPPoE 协议提供了在广播式网络上建立点对点会话的能力，并完成用户接入认证业务。

基于 PPPoE 的认证系统中，PPPoE 客户端到 PPPoE 服务器之间为二层网络，PPPoE 服务器负责终结 PPPoE 客户端发起的 PPPoE 协议报文，并利用 PPP 对客户终端的 PPP 连接请求进行认证。

PPPoE 认证可分为两个阶段 ，PPPoE 发现阶段和 PPPoE 会话阶段。在 PPPoE 发现阶段是用户终端在广播网络寻找接入服务器的过程（BRAS 设备），并确定会话标识 Session ID。 在 PPPoE 会话阶段，主机和接入服务器之间进行 PPP 的各项协商和数据传输，协商过程主要包括 LCP 协商、用户认证、NAC 协商三个过程。

PPPoE 认证可分为 PAP 和 CHAP 两种方式。以 CHAP 为例，用户接入认证流程如下：

图2-5 Portal 认证流程图



详细的流程说明如下：

2. PPPOE 客户端向 PPPOE 服务器设备（这里是 BRAS 设备）发送一个 PADI 报文，开始 PPPoE 接入。
3. PPPOE 服务器向客户端发送 PADO 报文。
4. 客户端根据回应，发起 PADR 请求给 PPPOE 服务器。
5. PPPOE 服务器产生一个 Session id，通过 PADS 发给客户端。

6. 客户端和 PPPOE 服务器之间进行 PPP 的 LCP 协商，建立链路层通信。
7. PPPOE 服务器通过 Challenge 报文发送给认证客户端,提供一个 128bit 的 Challenge。客户端收到 Challenge 报文后，将密码和 Challenge 做 MD5 算法后的，在 Response 回应报文中把它发送给 PPPOE 服务器。
8. PPPOE 服务器将 Challenge、Challenge-Password 和用户名一起送到 RADIUS 用户认证服务器，由 RADIUS 用户认证服务器进行认证。
9. RADIUS 用户认证服务器根据用户信息判断用户是否合法,然后回应认证成功/失败报文到 PPPOE 服务器。如果成功，携带协商参数，以及用户的相关业务属性给用户授权。如果认证失败，则流程到此结束。
10. PPPOE 服务器将认证结果返回给客户端。
11. 用户进行 NCP（如 IPCP）协商，通过 PPPOE 服务器获取到规划的 IP 地址等参数。
12. 认证如果成功，用户则成功接入网络。

2.2.6 四种认证方式比较

MAC 认证、802.1X 认证、Portal 认证和 PPPoE 认证对比如表 2-1 所示。

表2-1 认证方式对比

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，准入认证点在汇聚层或者核心层交换机上； 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。

在园区网 AAA 计费方案中，用户准入认证一般选择 802.1X、Portal 认证方式，用户准出认证可采用 Portal、PPPoE 等认证方式。

2.3 授权方案介绍

用户授权指用户认证通过，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。

用户授权方案主要有三种类型：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。

2.3.1 动态 VLAN 授权

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 VLAN 授权用于园区内网准入场景，方式通过切换 VLAN 改变用户的权限，不同 VLAN 的权限控制通过在接入层或者汇聚层交换机上部署 ACL 实现。

- 用户认证前，用户终端处于 Guest VLAN 中，访问权限受 Guest VLAN 限制。
- 用户认证通过后，如果用户终端不安全，则划分到隔离 VLAN 中，访问权限受隔离 VLAN 控制。
- 用户认证通过后，如果用户终端安全，则划分到业务 VLAN 中，访问权限受业务 VLAN 控制。

2.3.2 动态 ACL 授权

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。

动态 ACL 授权一般用于内网准入认证场景，需要服务器下发 ACL 给交换机，实现对用户访问权限的控制。准入服务器支持通过两种方式下发 ACL：

- 服务器上配置 ACL，并直接下发 ACL 内容至交换机。

  这种权限下发方式的优点在于 ACL 配置在服务器上，维护方便，缺点在于每个用户都占用不同的 ACL 资源，因而对接入交换机的 ACL 资源有较高的要求。
- 接入交换机上配置 ACL，服务器下发 ACL 号。

  这种权限下发优势是部署简单，服务器不需要做负载配置，但同时，由于权限的配置是在接入交换机上，当权限的具体内容需要修改的时候，需要和网管联动下发 ACL 规则内容。

2.3.3 基于用户组的授权方案

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。

基于用户组的授权方案主要有两个步骤：

- 用户组内容在网络准入设备上配置

包括优先级（Remark）、授权 ACL、授权 VLAN 等属性，可通过网管批量下发到准入设备上。

- AAA 服务器下发用户组到网络设备

  在用户认证通过后，AAA 服务器可以直接下发用户组名称到网络设备上。对于第一个用户，准入设备基于配置的用户组属性，下发安全策略，后续同一用户组用户上线，认证通过后直接加入对应用户组即可。

2.3.4 无线用户授权方式

无线用户的认证授权可以部署在交换机上，也可以在部署在 AC 上。

- 无线用户交换机上认证授权

  无线用户在交换机上授权时，可与有线用户统一认证和管理。

  - 无线接入采用 Open System 或 WEP 认证。
  - 用户通过代理在交换机上认证上线。

- 无线用户 AC 集中认证授权

  无线用户通过无线 802.1X 或者 Portal 方式在 AC 上认证并接入网络，。

  - 无线接入采用 802.1X 方式认证；
  - AAA 服务器通过用户组授权方式向无线用户下发权限。

2.4 计费方案介绍

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。

3 园区网 AAA 部署方案

3.1 园区网 AAA 方案选择

华为园区网 AAA 解决方案基于用户需求和应用场景不同，提供四套差异性解决方案共用户选择。四套方案园区网 AAA 方案对比如下：

表3-1 园区网 AAA 部署方案对比

编号	AAA 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，推荐 Portal 认证方式； 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。

3.2 计费网关一次认证方案

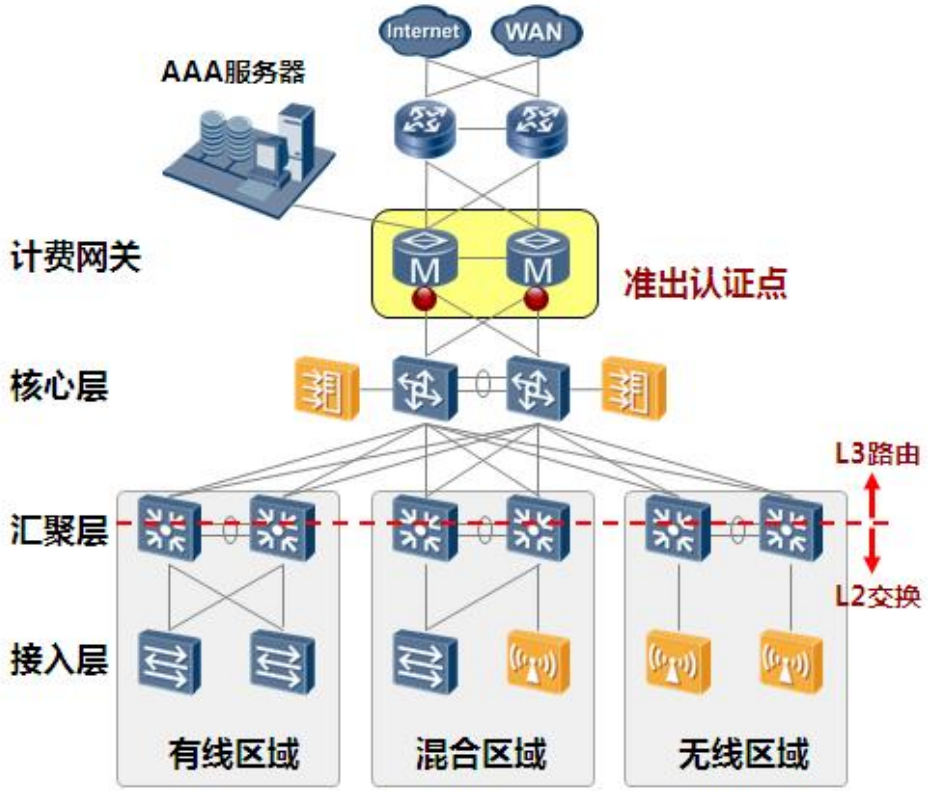
3.2.1 应用场景

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。

3.2.2 方案部署

计费网关一次认证方案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3-1 计费网关一次认证方案



二三层分界点规划

考虑到网络架构和设备转发能力，二三层推荐如下规划：

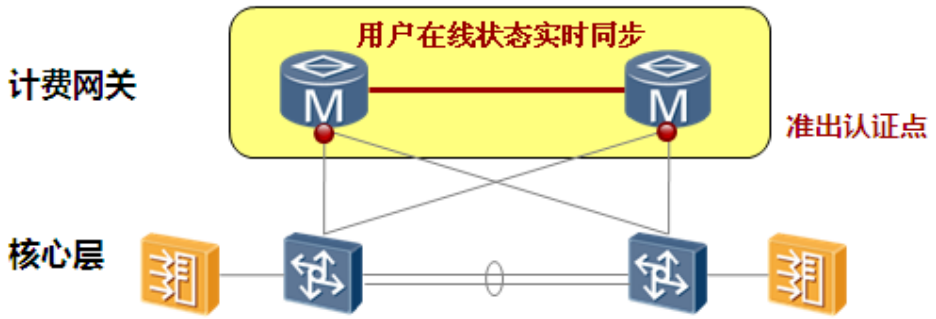
- 园区网网络如果为接入、汇聚、核心三层结构，则二三层分界点部署在汇聚层交换机上，如上图所示；
- 园区网络如果为接入、核心扁平化结构，则二三层分界点部署在核心层交换上。

计费网关双机热备

计费网关作为准出设备，部署在园区出口，只对出园区用户报文进行计费。计费网关可采用单机和主备两种部署方式，为了提升计费系统可靠性，推荐采用主备方式。

采用主备方式，计费网关可以做到用户数据实时同步。用户在任一设备上线后，在线信息会同步到对端设备，保证两台计费网关信息一致。

图3-2 计费网关一次认证方案



内网准入不做认证

本方案应用于中、小型规模运营园区，内网不做准入认证。

外网准出 Portal 认证

准出认证采用 Portal 认证方式，部署在计费网关上。用户上线后，从 DHCP 服务器获取到 IP 地址，可以自由访问内部网络。当访问任何网站时，用户的第一个 HTTP 报文重定向到 Portal 服务器，由 Portal 服务器推送认证页面，认证通过后获得特定访问权限。

网络安全规划

- 为防止用户间地址盗用、欺骗，可以在接入交换机上部署 DHCP snooping、IP Source Guard 等安全特性。
- 为有效限制接入终端和防止终端盗用，可以绑定用户或客户端到交换机端口。
- 为防止终端用户互访，可在接入交换机上部署端口隔离。

3.2.3 推荐产品

计费网关和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，计费网关选择 Srun 3000；
- 城市热点

  AAA 服务器选择城市热点 Dr.COM 系统，计费网关选择 Dr.COM 2166。

3.2.4 客户价值

计费网关一次认证方案主要客户价值如下：

- 计费网关一次认证，主备方式按需选择，方便管理维护。
- 准出 Portal 认证，无需安装客户端，提升用户体验。

3.3 准入准出认证分离方案

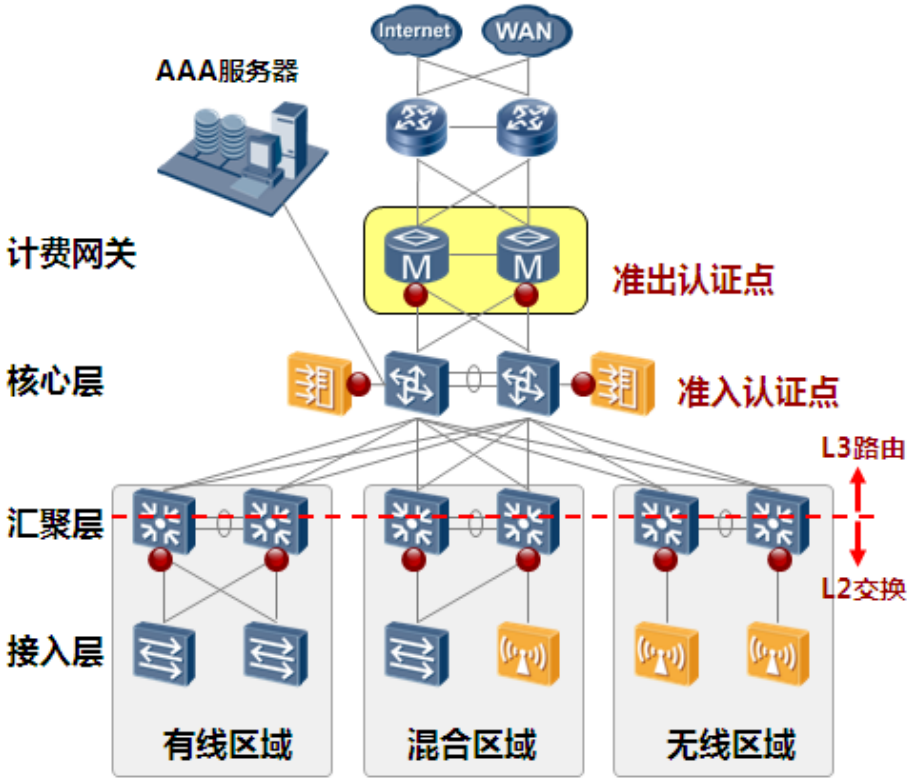
3.3.1 应用场景

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。

3.3.2 方案部署

计费网关一次认证方案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3-3 准入准出认证分离方案



二三层分界点规划

考虑到网络架构和设备转发能力，二三层推荐如下规划：

- 园区网网络如果为接入、汇聚、核心三层结构，则二三层分界点部署在汇聚层交换机上，如上图所示；
- 园区网络如果为接入、核心扁平化结构，则二三层分界点部署在核心层交换上。

计费网关双机热备

计费网关作为准出设备，部署在园区出口，只对出园区用户报文进行计费。计费网关可采用单机和主备两种部署方式，为了提升计费系统可靠性，推荐采用主备方式。

采用主备方式，计费网关可以做到用户数据实时同步。用户在任一设备上线后，在线信息会同步到对端设备，保证两台计费网关信息一致。

内网准入认证

本方案用户对于内网安全具有较高要求，部署内网准入认证，认证方式可选择 802.1X 认证或者 Portal 认证。

- 内网准入 802.1X 认证

802.1X 认整属于二层认证，用户 IP 地址认证成功后分配，控制点可放在接入层或者汇聚层交换机上，安全性高于 Portal 认证，但需要客户端。

- 内网准入 Portal 认证

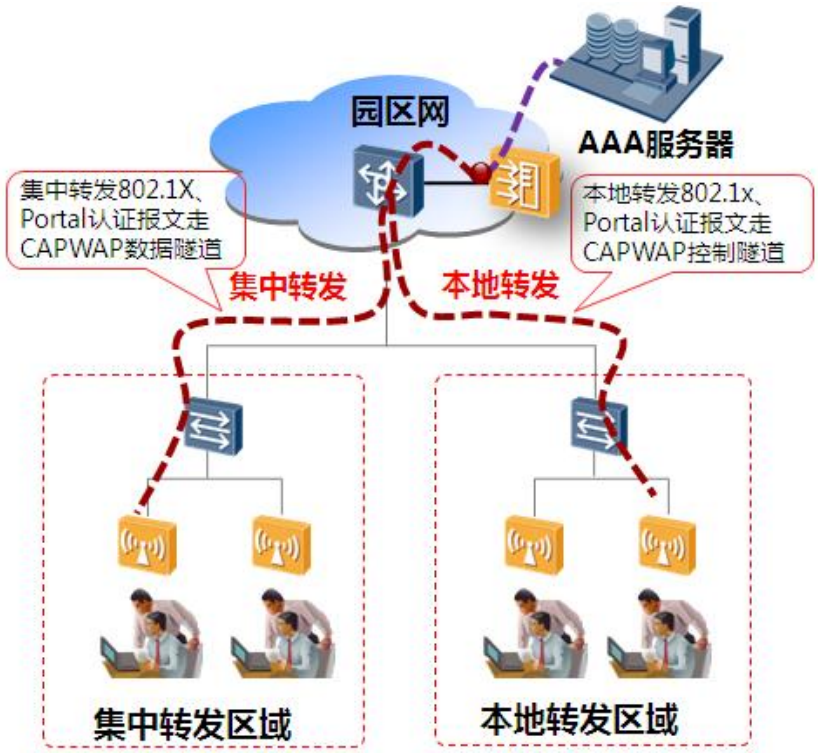
Portal 认证属于三层认证，用户 IP 地址在认证前分配，一般部署在网关设备上，安全性适中，但无需客户端配合。

具体认证方式选择上，如果用户对于安全准入有较高要求，可选择具有客户端的 802.1X 认证；如果用户追求方便运维，特别是存在智能终端接入的园区中，可推荐内网采用 Portal 认证方式。

无线用户集中认证

无线用户集中认证，可以提供将 AP 及无线用户统一管理，能为无线用户提供认证和授权，保障无线用户接入的安全。

图3-4 无线用户 AC 集中认证



无线用户 AC 集中认证方案可采用二层组网或三层组网方式。一般而言，在大、小型园区都采用三层组网方式。

AP 的转发模式可以采用集中转发模式和本地转发模式两种。

- 采用集中转发模式时，WLAN 管理报文与数据报文都通过 CAPWAP 隧道在 AP 与 AC 之间传输。
- 采用本地转发模式时，仅管理报文通过 CAPWAP 隧道在 AP 与 AC 之间传输，数据报文由 AP 直接进行转发。

说明

在 AP 进行本地转发时，可以通过配置使 EAP、Portal 报文进入 CAPWAP 控制隧道，从而上送到 AC 设备，完成认证过程。

此方案的优点在于：

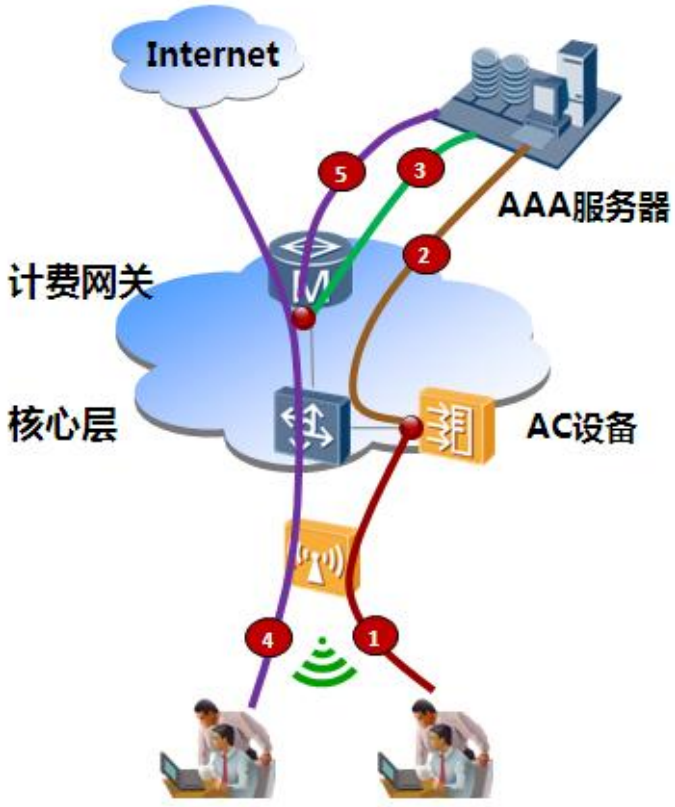
- 增强用户控制能力：认证点和控制点分离，授权到 AP；
- 解决漫游权限切换：无线用户集中管理，解决漫游场景下用户跨 AP 权限切换问题。
- 发挥本地转发优势： 本地转发场景下，无线用户在 AC 集中认证，数据流量不经过 AC，可使用户安全和网络性能做到完美结合。

外网准出 Portal 认证

准出认证部署在计费网关上，由于跨越三层设备，采用 Portal 认证方式。

以无线用户认证为例，说明本方案中准入、准出一体化认证的流程。在图中，AAA 服务器集成 Portal 服务器功能。

图3-5 准入准出认证流程



（1）用户访问网页，重定向到内网认证 Portal 页面，要求用户输入用户名和密码；

（2）AAA 服务器通过 Radius 协议，和准入认证设备 AC 进行协商，打开内网准入权限；

（3）如果用户在 Portal 认证页面同时选择访问外网，则 AAA 服务器通知计费网关，开启准出认证权限；

（4）后续用户可直接访问 Internet 等外网资源，无需再次登陆认证；

（5）计费网关基于时间或者流量进行访问统计，并上送 AAA 服务器进行计费；

实际登陆中，用户可以选择准入准出一次认证，也可以选择只登陆内网。

网络安全规划

- 为防止用户间地址盗用、欺骗，可以在接入交换机上部署 DHCP snooping、IP Source Guard 等安全特性。
- 为有效限制接入终端和防止终端盗用，可以绑定用户或客户端到交换机端口。
- 为防止终端用户互访，可在接入交换机上部署端口隔离。

3.3.3 推荐产品

计费网关和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，计费网关选择 Srun 3000；
- 城市热点

  AAA 服务器选择城市热点 Dr.COM 系统，计费网关选择 Dr.COM 2166。

3.3.4 客户价值

准入、准出认证分离方案主要客户价值如下：

- 准入准出分离控制，内网准入接入，增强网络安全性；
- 准入准出一次认证，输入一次密码，提升用户体验。

3.4 IPv4/IPv6 双协议栈方案

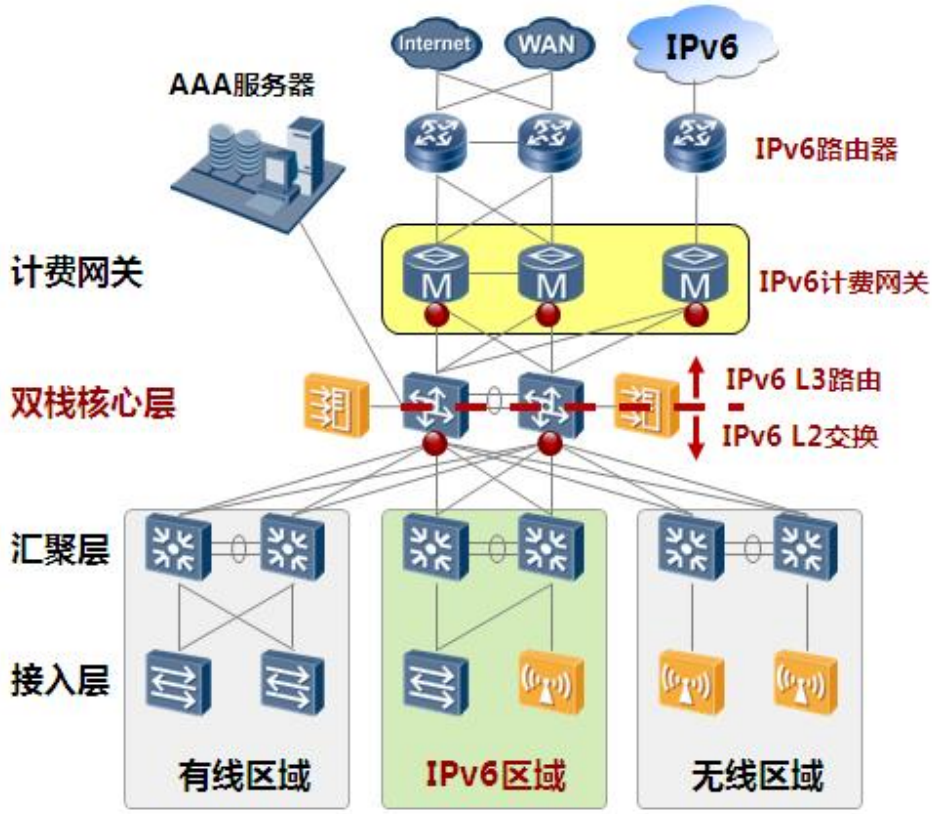
3.4.1 应用场景

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。

3.4.2 方案部署

对于部署 IPv4/IPv6 双栈方案的园区网，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3-6 IPv4/IPv6 双协议栈方案



二三层分界点规划

考虑到网络架构和设备转发能力，IPv6 网络二三层推荐如下规划：

- 如果核心层交换机支持双协议栈，IPv6 网关可部署在核心层，如上图示例；
- 如果汇聚层交换机支持双协议栈，则 IPv6 二三层分界点可部署在汇聚层交换机上。

计费网关分离热备

对于 IPv4 和 IPv6 共存的园区，计费网关推荐分离部署：

- IPv4 用户占据园区主要流量，为了提升计费系统可靠性，推荐采用主备方式。采用主备方式，计费网关可以做到用户数据实时同步。
- 对于 IPv6 网络，可单独部署计费网关，IPv6 用户的准出认证点在计费网关上。

内网准入认证

本方案用户对于内网安全具有较高要求，部署内网准入认证，一般 IPv6 和 IPv4 用户认证方式保持一直，可选择 802.1X 认证或者 Portal 认证。

- 内网准入 802.1X 认证

802.1X 认整属于二层认证，用户 IP 地址认证成功后分配，控制点可放在接入层或者汇聚层交换机上，安全性高于 Portal 认证，但需要客户端。

- 内网准入 Portal 认证

Portal 认证属于三层认证，用户 IP 地址在认证前分配，一般部署在网关设备上，安全性适中，但无需客户端配合。

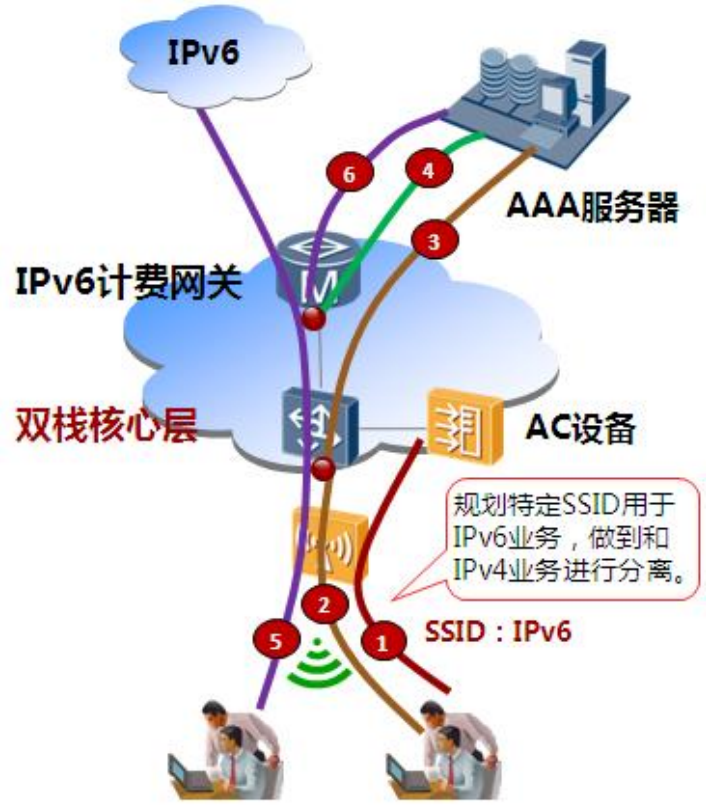
具体认证方式选择上，如果用户对于安全准入有较高要求，可选择具有客户端的 802.1X 认证；如果用户追求方便运维，特别是存在智能终端接入的园区中，可推荐内网采用 Portal 认证方式。

外网准出 Portal 认证

准出认证部署在计费网关上，由于跨越三层设备，采用 Portal 认证方式。

以无线 IPv6 用户认证为例，说明本方案中准入、准出一体化认证的流程。在图中，AAA 服务器集成 Portal 服务器功能。无线用户采用本地转发，IPv6 业务规划专有 SSID。

图3-7 IPv6 用户准入准出认证流程



（1）无线终端首先和 AC 建立无线链路关联，链路关联不做认证；

（2）用户访问网页，重定向到内网认证 Portal 页面，要求用户输入用户名和密码；

（3）AAA 服务器通过 Radius 协议，和核心交换机进行协商，打开内网准入权限；

（4）如果用户在 Portal 认证页面同时选择访问外网，则 AAA 服务器通知 IPv6 计费网关，开启准出认证权限；

（5）后续用户可直接访问 Internet 等外网资源，无需再次登陆认证；

（6）计费网关基于时间或者流量进行访问统计，并上送 AAA 服务器进行计费。

实际登陆中，用户可以选择准入准出一次认证，也可以选择只登陆内网。

网络安全规划

- 为防止用户间地址盗用、欺骗，可以在接入交换机上部署 DHCP snooping、IP Source Guard 等安全特性。
- 为有效限制接入终端和防止终端盗用，可以绑定用户或客户端到交换机端口。
- 为防止终端用户互访，可在接入交换机上部署端口隔离。

3.4.3 推荐产品

计费网关和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，计费网关选择 Srun 3000；
- 城市热点

  AAA 服务器选择城市热点 Dr.COM 系统，计费网关选择 Dr.COM 2166。

3.4.4 客户价值

IPv4./IPv6 双协议栈方案主要客户价值如下：

- 双栈网络计费网关独立部署，提升网络可靠性；
- 双栈用户一个帐号，AAA 服务器集中管理，提升用户体验。

3.5 大二层园区网计费方案

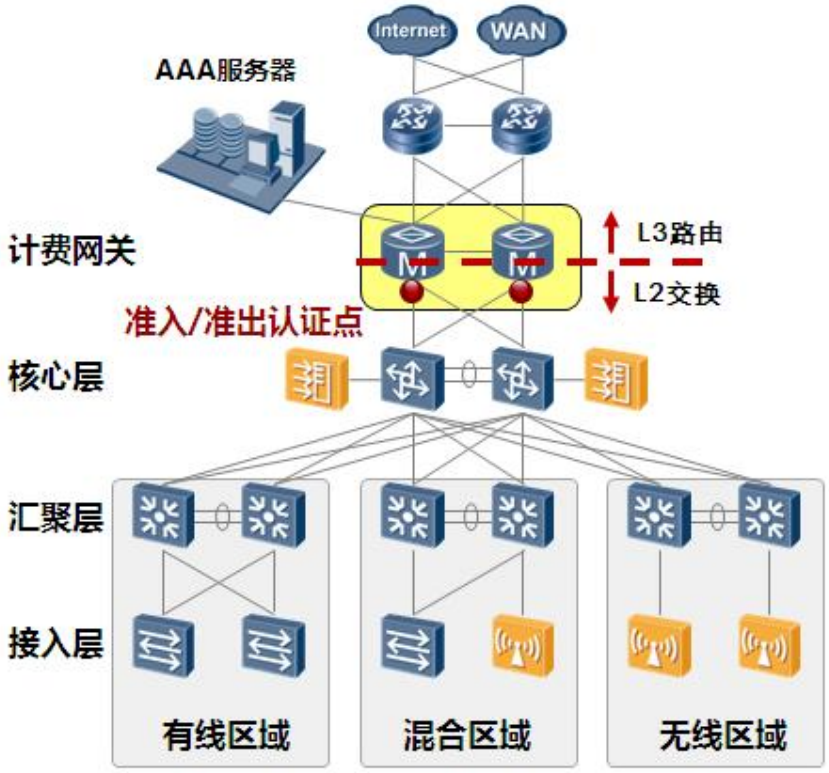
3.5.1 应用场景

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

3.5.2 方案部署

在该网络拓扑方案中，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。

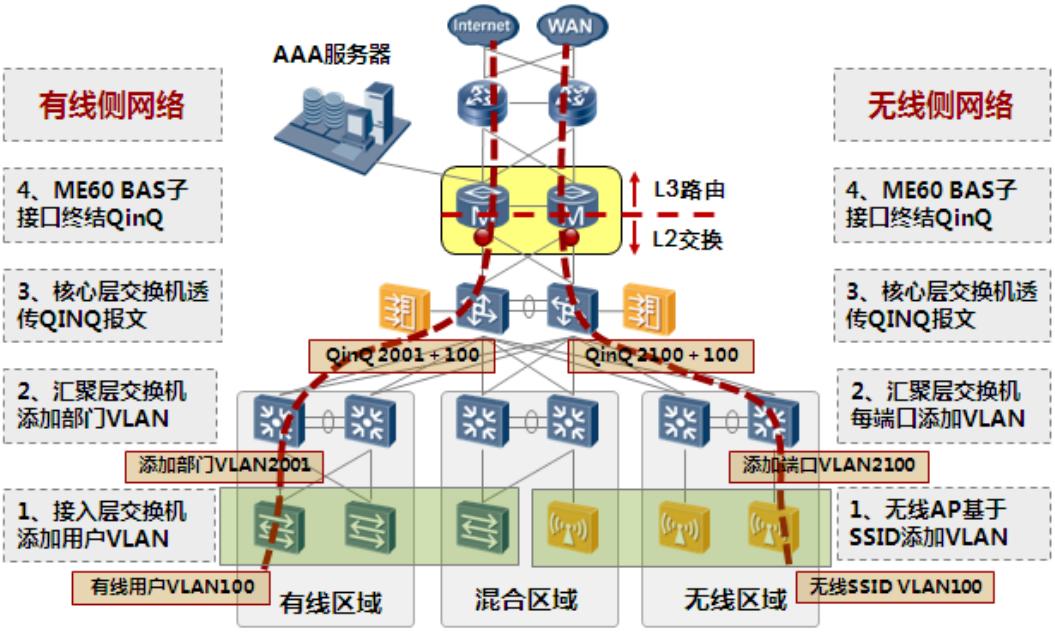
图3-8 大二层园区网计费方案



二三层分界点规划

本方案中，由于 BRAS 设备具有强大的转发性能，故二三层分界点上移，部署在计费网关上。整个园区基于 BRAS 设备构建大二层园区，VLAN 规划如下图：

图3-9 有线和无线网络 VLAN 规划



具体部署上，接入层交换机每端口添加用户 VLAN，汇聚层交换机添加部门 VLAN，核心层交换机透传 QINQ 报文，ME60 作为园区网关，结结 QinQ 报文。

计费网关双机热备

计费网关作为准出设备，部署在园区出口，只对出园区用户报文进行计费。计费网关可采用单机和主备两种部署方式，为了提升计费系统可靠性，推荐采用主备方式。

采用主备方式，计费网关可以做到用户数据实时同步。用户在任一设备上线后，在线信息会同步到对端设备，保证两台计费网关信息一致。

准入准出一体化认证

本方案认证点部署在 BRAS 设备 ME60 上，兼具内网、外网控制能力。

- 内网准入控制

通过 QinQ 隔离内部园区，网关部署在计费网关上，这样园区用户只有通过出口的认证后，才能访问园区内网的服务器资源。

- 外网准出控制

如果用户需要访问外网，则在计费网关上打开外网访问权限，访问 Internet。

具体部署中，认证方式可以选择 Portal 认证或者 PPPoE 认证。

- Portal 认证

对于智能手机、平板电脑等智能终端，一般不需要安装客户端，可选择 Portal 认证，方便用户随时随地接入。

- PPPoE 认证

对于可以安装客户端的终端，如普通 PC，可以采用 PPPoE 认证。

DAA 实现内网外网分离计费

ME60 特有的 DAA（Destination Address Accounting）功能，可以实现对用户接入不同访问目的地的差别化控制和计费。

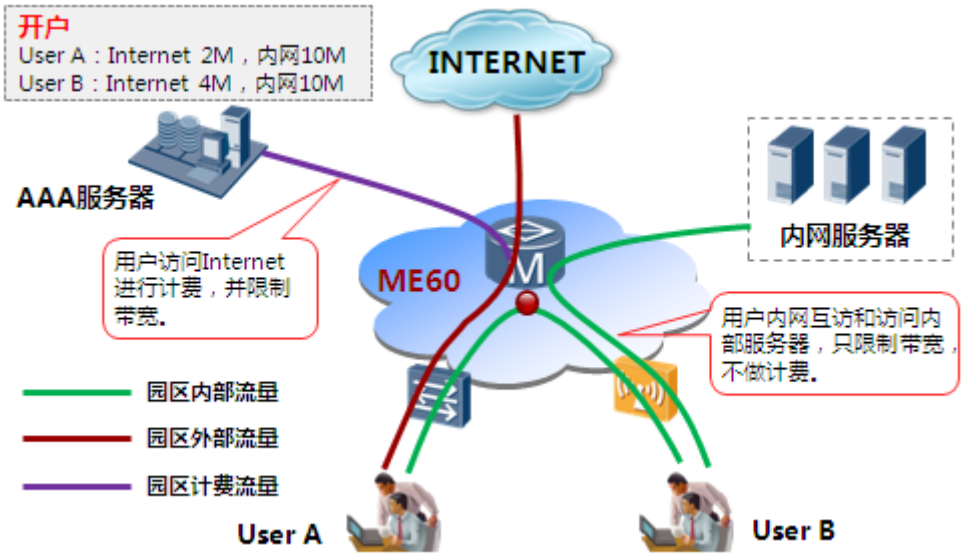
- 按目的地址实施带宽策略

DAA 实现园区内网、外网分离控制，并实施不同的带宽策略。例如，对于 User A，可以控制访问内网带宽为 10M，访问 Internet 带宽为 2M。

- 按目的地址实施计费策略

DAA 实现不同网络通道独立进行流量统计，只对外网访问流量进行计费。例如，对于 User A，访问内部服务器、和其他用户互访流量不做计费，而访问 Internet 流量进行基于时间或者流量的费用计算。

图3-10 DAA 实现内网外网分离计费



网络安全规划

- 为防止用户间地址盗用、欺骗，可以在接入交换机上部署 DHCP snooping、IP Source Guard 等安全特性。
- 为有效限制接入终端和防止终端盗用，可以绑定用户或客户端到交换机端口。
- 为防止终端用户互访，可在接入交换机上部署端口隔离。

3.5.3 推荐产品

本方案中，计费网关选择 BRAS 设备 ME60，服务器系统选择合作方产品：

- 深澜软件

  AAA 服务器选择深澜软件 Srun 系统；
- 城市热点

  AAA 服务器选择城市热点 Dr.COM 系统。

3.5.4 客户价值

大二层园区网计费方案主要客户价值如下：

- 业界最高性能 BRAS 设备构建大二层园区网，准入准出一体化认证，方便管理维护。
- DAA 机制按地址计费，提供创新的商业模式。

4 产品建议

对于园区网 AAA 解决方案所涉及的各节点和网元，华为公司推荐使用的产品如下：

表4-1 部件产品建议表

部件	产品/型号
接入交换机	S5700、S3700、S2700、S1700
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
接入路由器	AR3200、AR2200、AR1200
高端路由器	NE40E
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