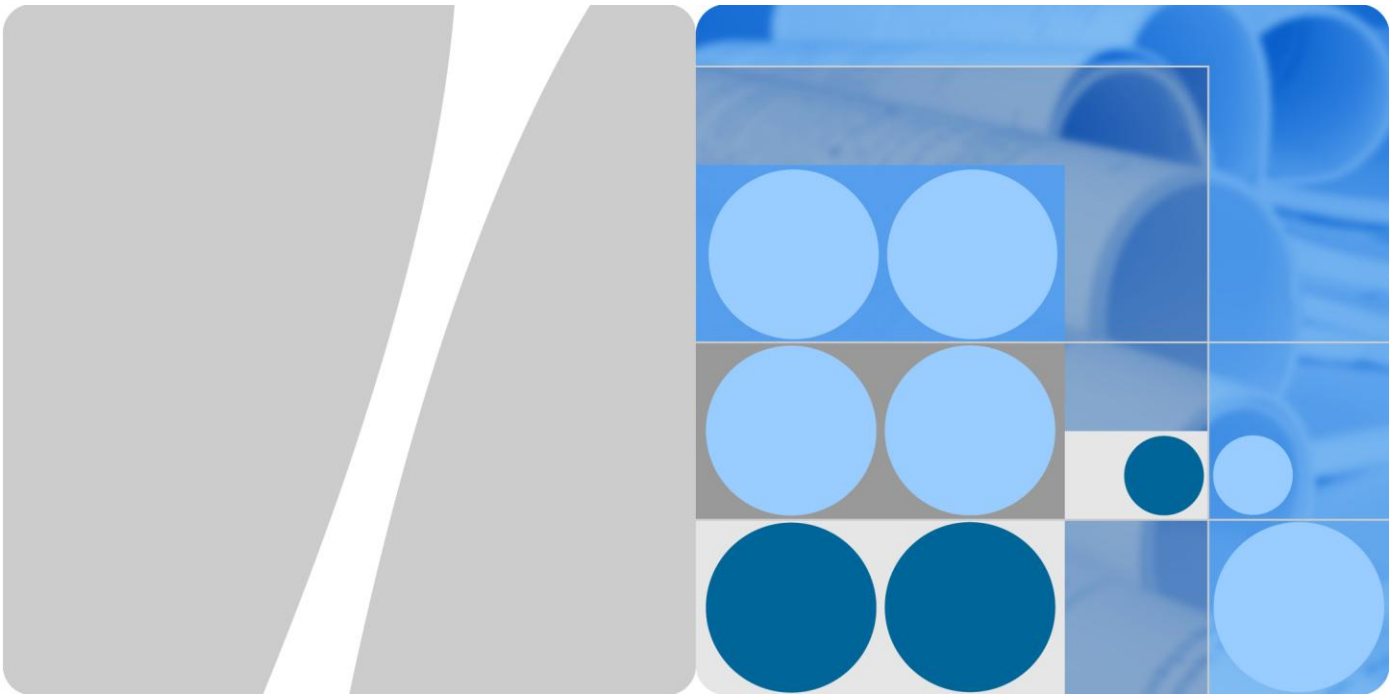

华为 AR G3 企业路由器

BRAS 技术白皮书

文档版本 V1.0

发布日期 2013.12.15

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

目 录

插图目录

1 BRAS 特性简介

1.1 BRAS 业务概述

1.1.1 引入背景

随着 Internet 市场的不断发展，人们对通信的需求已从传统的电话、传真、电报等低速业务逐渐向高速的 Internet 接入、可视电话、视频点播等宽带业务领域延伸，用户对上网速率的需求越来越高，传统拨号 Modem 的低速上网方式已无法满足用户需求。

与此同时，接入到城域网的用户越来越多，用户的业务需求也日益膨胀，宽带城域网面临着向多业务承载网方向的发展趋势。在这种情势下，如何对这些接入用户进行有效的管理，使之能够对用户接入的合法性进行验证？如何对用户使用的业务进行管理与控制，以防止接入用户对网络带宽、IP 地址等网络资源的占用不受任何约束与控制，从而使各类业务能够精细运营？这些均成为运营商们密切关注的问题。

由此产生了 BRAS（Broadband Remote Access Server），即宽带接入服务器。BRAS 具有灵活的接入认证方式、有效的地址管理功能、强大的用户管理功能，并能提供丰富灵活的业务及控制功能，与公司的其他通信产品组合在一起，即可提供一个“可管理、可运营、可盈利”的宽带城域网解决方案。

1.1.2 网络定位

1.1.2.1 宽带城域网

宽带 IP 城域网主要由三个网络层次构成：接入层、汇聚层和核心层。根据网络规模和应用不同，网络层次可能增多或减少，各层网络设备规格也可能会有所差异，如图所示。

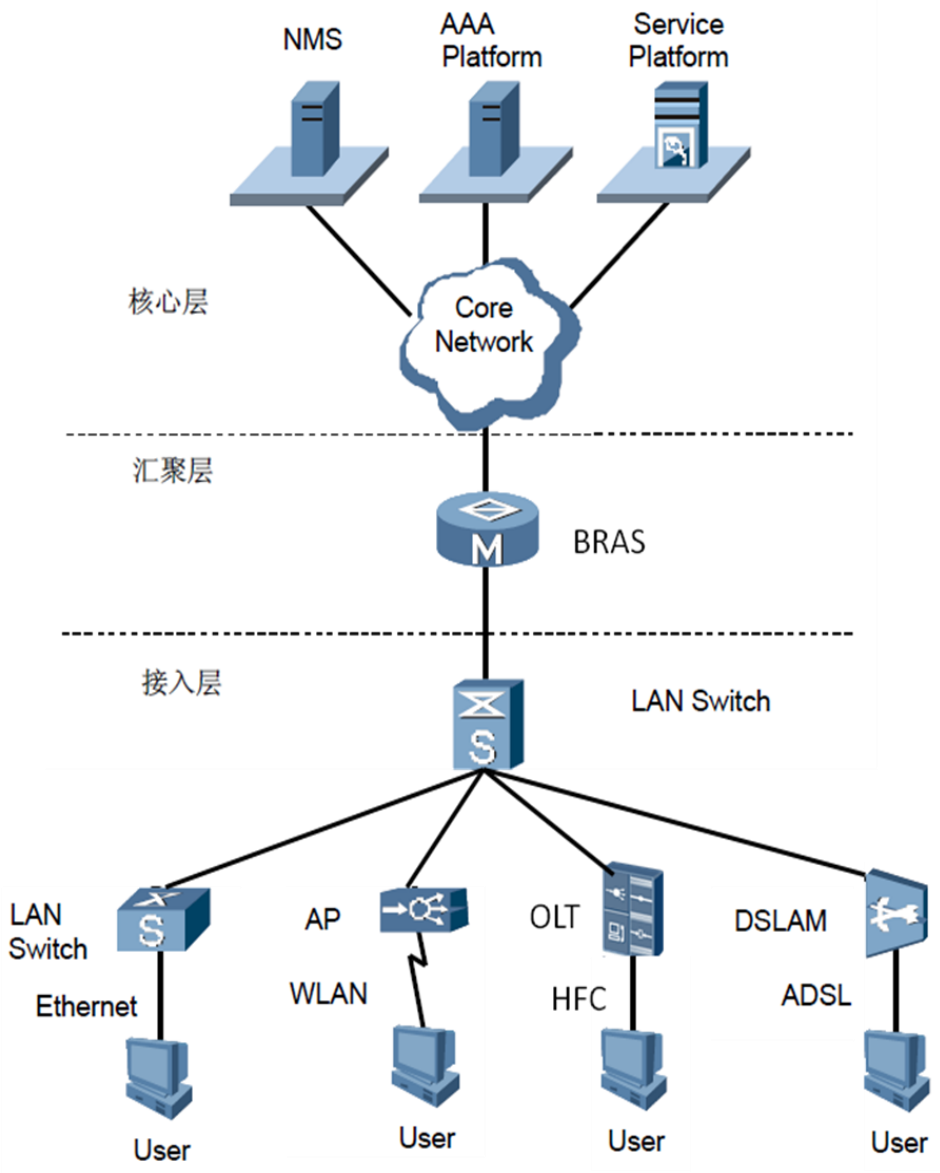

图1-1　　宽带城域网示意图

接入层：

接入层的主要功能是完成用户流量的汇聚和隔离，即把用户流量集中到汇聚层，并却能够保证接入层设备不会成为用户的小交换机。同时感知接入线路状态及参数，并将其上报给汇聚层；实施汇聚层下发的线路控制策略、OAM 检测。对于以太接入用户，可以通过低端的二层或者三层交换机接入。用户可以通过五类双绞线接入交换机，也可以通过在双绞线上使用 VDSL（Very-high-bit-rate Digital Subscriber Loop）技术接入到交换机。对于 ADSL 用户，可以通过 IP DSLAM（Digital Subscriber Line AccessMultiplexer）设备提供 IP 上行口，接入 IP 城域网。广电网络双向网络改造，用户通过 HFC

（Hybrid Fiber－Coaxial 混合光纤同轴电缆网）接入到 OLT 设备（optical line terminal 光线路终端），OLT 通过交换机接入到汇聚层。

汇聚层：

汇聚层设备主要完成用户业务的分发、汇聚，提供用户管理、业务控制，网络安全及认证计费等功能。根据网络规模和应用不同，设备可以放在小区中心或端局。

核心层：

核心层设备的主要功能是为整个网络提供一个路由和交换平台，对设备的吞吐量和可靠性有很高要求，所以一般由 GSR（Gigabit Switching Router）或者大容量三层交换机承担。

NE16EX 作为 BRAS 设备时，定位于宽带城域网的边缘汇聚层。在这里，NE16EX 不仅担当着各类宽带接入用户的认证、计费网关，还担当着用户的业务控制网关。它能够为用户提供多种宽带接入业务和丰富的增值业务，并能够对用户使用的业务进行带宽、流量监管、QoS 等方面的控制。

1.1.2.2 校园网

随着宽带互联网的飞速发展，多数高校都建成了覆盖教室、图书馆、师生公寓、办公楼的校园网，有的甚至还部署了 wlan，实现了校园网接入的无缝覆盖，为师生提供高速互联网接入服务，校园网在很大程度上已不再是一个小的局域网，就其用户规模来说，可能相当于一个区域网甚至市级网，因此校园网可运营的理念应运而生，以适应现代校园网“以网养网”的需求。

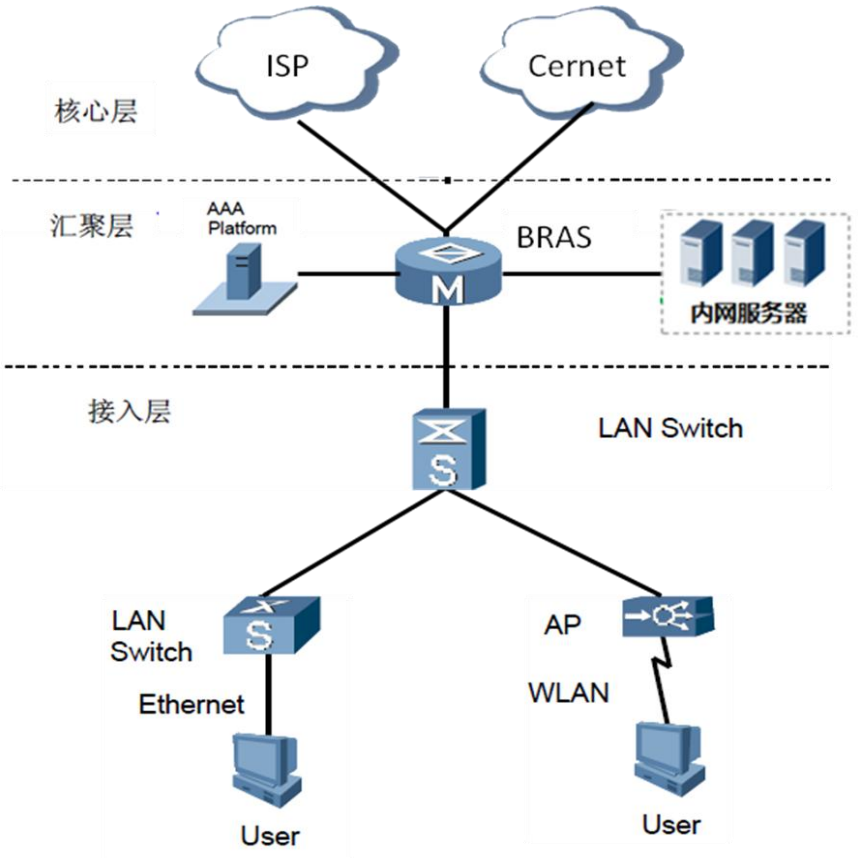

图1-2　　校园网

校园网具有可运营的特点，但与基础电信运营商的网络运营业务相比又有着鲜明的特殊性：

- 网络构成相对复杂，公共服务网络和部分运营网络共存。
- 用户规模大且主要集中在校园内，一般为在校大学生和教师。
- 上网时段相对集中，主要集中在课余时间，网络高峰时段相对固定，同时存在突发流量大的特性。
- 网络应用需求多样，主要是消耗带宽的新技术（如bt等p2p软件）。
- 网络管理难度大，一是计算机病毒、盗版资源泛滥；二是大学生大都处于20岁左右的年龄阶段，非法、不健康的网络不良行为突发性高。

1.1.3 系统架构

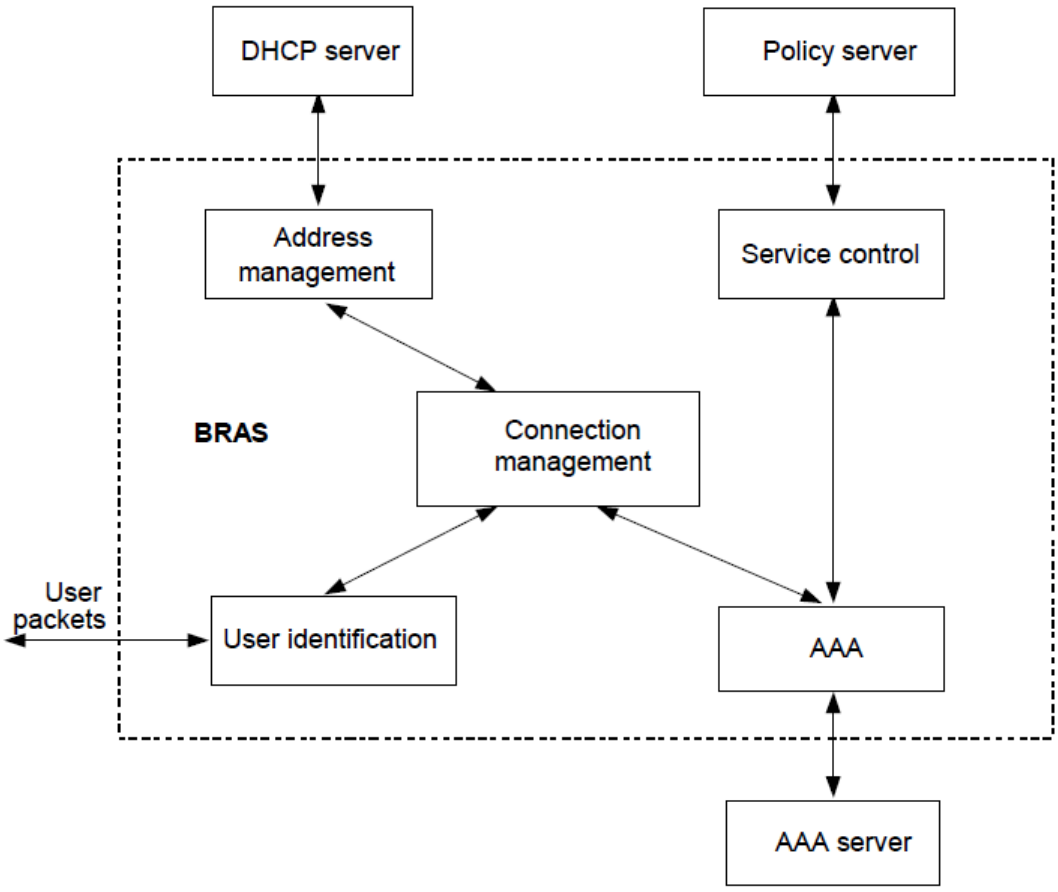

图1-3　　BRAS 体系系统架构

BRAS 系统共有如下几个功能部件：

- 用户接入识别

  主要完成对用户各种接入协议报文的识别与处理、在用户认证过程中获取用户的物理信息以及用户名和密码，从而为实现用户接入提供信息依据和安全保障。

- 连接管理

  BRAS 的核心组件，它负责协调接入识别、地址管理、AAA 和用户管理等组件之间的交互关系，协助完成用户连接的建立、维护及拆除等功能。

- AAA 及用户管理

  AAA 是Authentication（认证）、Authorization（授权）和Accounting（计费）的简称。认证是识别用户身份的过程；授权是根据认证识别后的用户情况授予对应的网络使用权限，包括QoS（Quality of Service）、带宽控制、访问权限、用户策略等；计费是根据认证后的用户身份采用对应的计费策略并记录、提供计费信息（时长、流量、位置等）。

- 地址分配与管理

  负责为接入用户分配IP 地址，并对用户IP地址进行管理，以确保IP地址资源得到合理使用。

- 业务控制

  负责对用户接入业务和增值业务进行访问权限、带宽、QoS等的控制。

- 外部服务器

  为便于运营商统一管理资源，BRAS需要与其他通信设备配合实现其功能，这些通信设备包括：

  - DHCP（Dynamic Host Configuration Protocol）服务器，负责为用户分配IP 地址。
  - AAA 服务器，如RADIUS（Remote Authentication Dial In User Service）服务器、HWTACACS（HuaWei Terminal Access Controller Access Control System）服务器，负责对接入用户进行认证、授权、计费。
  - 策略服务器，如RADIUS服务器，负责为用户下发业务策略。

用户接入识别、AAA 及用户管理、地址分配与管理、业务控制等功能部件在连接管理组件的控制协调下，并在外部服务器配合下，实现各种宽带用户的接入管理及业务控制。

1.1.4 业务基本流程

BRAS 业务基本处理流程如下所述：

1. 用户发出连接请求报文到达 BRAS 后，BRAS 的接入识别组件负责处理用户报文，从中提取用户的物理位置信息并判断是否允许接入，如果允许接入则向连接管理组件发用户连接请求。

2. 连接管理组件根据接入限制等条件判断是否允许用户接入，如果允许用户接入，给接入识别组件回应成功。

3. 接入识别组件接到连接管理组件成功回应后，通知用户，用户向接入识别组件发认证请求报文，接入识别组件从报文中提取用户名等认证信息，将认证信息打包后发送给连接管理组件要求认证。

4. 连接管理组件将来自接入识别组件的认证请求转发给 AAA 及用户管理组件。

5. AAA 及用户管理组件根据认证方案、授权方案进行认证和授权，然后将认证结果连同授权信息回应给连接管理组件。

6. 如果认证成功，连接管理组件向地址分配与管理组件申请 IP 地址。

7. 地址分配与管理组件根据用户的地址池信息，采用相应的地址分配策略分配 IP 地址（远端地址需要到外部的 DHCP 服务器分配），并将分配结果回应给连接管理组件。

8. 连接管理组件将认证结果连同 IP 地址一起回应给接入识别组件，接入识别组件与用户交互后，用户即可上线。

9. 用户上线后，AAA 及用户管理组件、业务控制组件共同负责对用户使用的基本业务、增值业务进行计费、带宽限制、QoS 等控制。

1.2 小型 BRAS 场景分析

1.2.1 广电宽带双向网络改造

广电宽带，通常是各地有线电视网络公司（台）负责运营的，通过 HFC（光纤+同轴电缆混合网）网向用户提供宽带服务，通过 CableModem 连接到计算机，理论到户最高速率 38M，实际速度要视网络具体情况而定。而电信网是使用 ADSL 模式使用电话线连接到用户。

广电网络公司正处在网络发展的第二阶段，完善网络结构，提高网络的承载力，采用多种技术方案实现网络双向化改造， 同时以多功能业务拓展和提高服务水准，来推动网络系统建设，使有线电视网络真正具有宽带、双向、多功能的承载能力，把普通老百姓的电视接收终端变成家庭多媒体信息终端。

2007 年全国各地开始数字电视整体转换工作，实现发展的第一阶段：广播式数字电视业务。通过第一阶段广播式数字电视节目业务的运营，广电网络确立了主营业务的品牌，建立并完善了业务服务运营平台， 发展了一定规模的机顶盒用户，建立了统一的用户管理和收费系统。但数字电视整体转换结束后，经过实际用户回访调查，用户对数字电视的满意程度却不高，用户已不满足于被动的收看电视节目，还希望能够通过手中的遥控器来选择与众不同、更加符合个人爱好、更具深度的信息，这就是个性化、专业化、多样化。在这个背景之下，互动电视、宽带业务，其它增值业务应运而生，广电网络的发展正进入第二阶段：开展宽带业务、互动增值业务。要开展这些宽带、互动增值业务就会涉及到双向网络改造、设备选型等一系列问题。

2013 年重庆广电进行宽带接入改造，提供 PPPoE 用户和 Web 用户的宽带接入，本地（区县）进行认证，远端（市局）计费。并发用户量支持 2K—10K。以各区县为站点，BAS/服务器和安全产品打包集成。重庆全市辖 38 个区县，有几个已采用软 BAS 完成了改造，剩余 27 个待实施。NE16EX 路由器填补了中小型 BRAS 设备市场空白，为广电提供宽带接入特性。

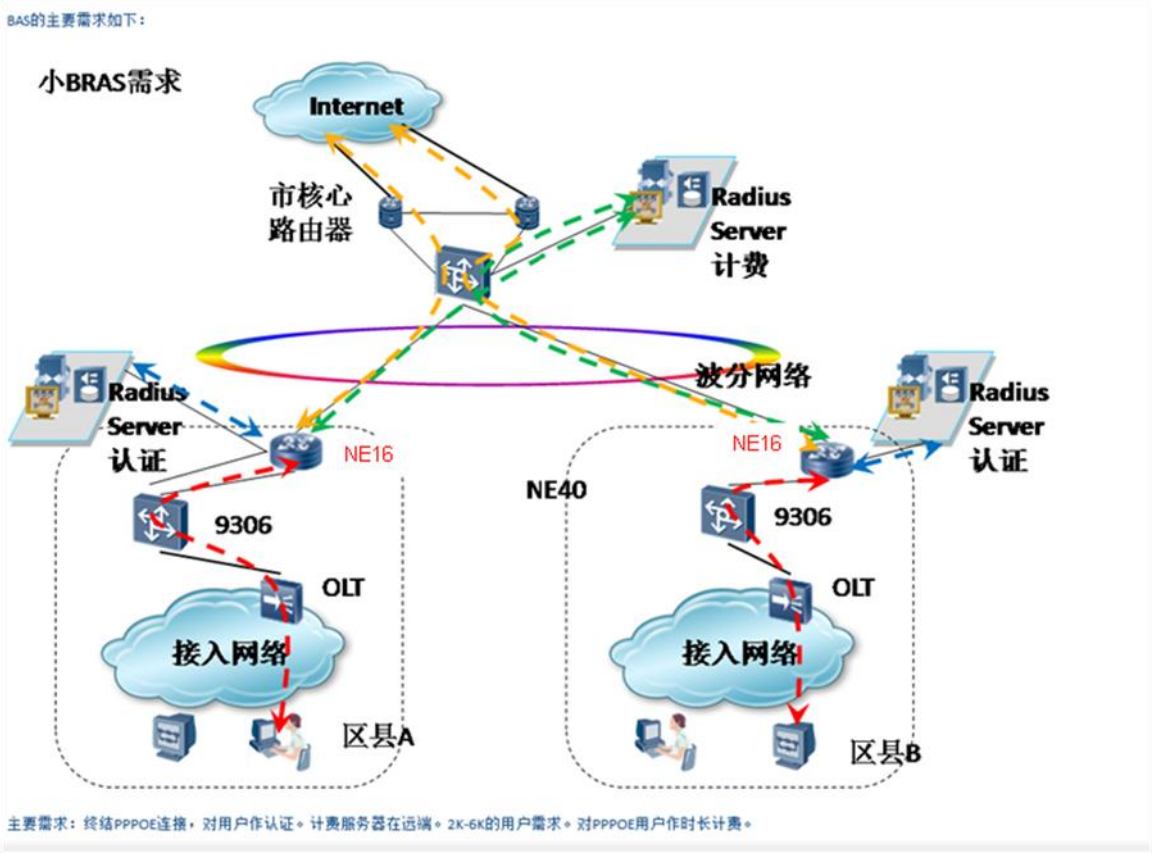

图1-4　　重庆广电小 BRAS 需求网络拓扑

1.2.2 园区网建设面临的问题

校园网运营管理面临的主要问题：

- 校园网进行无线网络建设，WLAN AC 设备和 BRAS 设备分别管理无线和有线用户，无法集中管理。
- 校内用户私接代理情况比较普遍，容易造成费用流失。
- cernet和internet同时接入，需要提供区别服务。
- 教师和学生往往要区别收费，需要提供灵活的计费方式。
- 网络internet出口容易出现拥塞，需要对带宽分配进行有效管理。
- 计费数据采集困难，对运营管理带来难度。
- 网络不良行为，非法网站访问控制困难，无法进行有效的记录。
- 校园分支和总部通过 VPN 安全互访。
- IPv6 过渡问题，CERNET2 是中国下一代互联网示范工程 CNGI 最大的核心网和惟一的全国性学术网，也是目前世界上规模最大纯 IPv6 互联网骨干网。

针对校园网自身的特点和运营管理中存在的主要问题，采用合理的认证计费和带宽限速策略是校园网运营的基本保障。

校园网管理的特点：

- 独特的计费方式。

  从校园网自身的特点来看，用户使用ftp、bt下载或者网络游戏、在线视频等频率很高，可能导致出口带宽占用太多，浏览网页等普通应用速度很慢，因此，通常学校会采用通过流量计费的方式来限制大流量的发生。并且，Cernet的现行收费政策是对教育网内免费，其他网络收费。因此，学校一般会要求对校园网用户出口访问能够区分不同的流量并且进行准确的记录，以收取相应的费用。

- 多个网络出口的需求。

  早期国内各高校一般通过中国教育科研网（cernet）接入internet。近年来，许多学校基于带宽的考虑，都在cernet出口的基础上，同时接入基础电信运营商公网的专线。这样，校园网就存在着多个网络出口，访问不同资源的流量通过不同的出口，这些出口可能使用不同的计费方式和费率策略。

- 接入方式多样化。

  校园网里存在着多种多样的接入方式。例如：pppoe、dhcp、l2tp、dot1x、web等，最后通过路由器接入internet。学校一般要求对这些不同接入方式的用户进行统一管理。

- 用户层次多样化。

  校园网用户的种类很多，如教师、学生、校长，甚至包含一些校办企业。这些不同的用户对网络服务的需求和收费标准都不一样。这就要求计费管理系统能够为不同的用户提供不同层次的服务，并制定不同的收费策略。

- 付费类型多样化。

  很多校园里都是采用预付费或预付费卡的方式。但对于一些特殊用户，也可能采用后付费或包月的方式。 账务管理相对简单。校园网一般都没有进行商业运营，对营账系统的要求简单。基于校园网计费管理的特点，建议对校园网的计费策略是内网免费，出口按照流量计费。

1.3 NE16EX 一体化 BRAS 解决方案

1.3.1 NE16EX BRAS 功能简介

针对广电网络双向改造和校园网目前现状，NE16EX 路由器提供了一体化 BRAS 解决方案。

NE16EX 目前支持的功能包括：

- 多核转发平台，高性能用户转发；
- 用户侧接口二层以太高密交换版板卡，三层以太板卡，
- 主控集成 WLAN AC；
- 支持多种认证方式，包括 MAC 认证、802.1X 认证、Portal 认证、PPPoE 和 L2TP 用户接入认证；
- 支持 RADIUS 和 HWTACACS 协议；
- 支持用户管理和地址管理；
- 支持按时长计费、按流量计费、包月计费等多种计费模式；
- 支持按照目的地址计费（DAA）；
- 支持配合 Radius 服务器进行在线用户管理（COA）；
- 用户日志管理；

1.3.2 NE16EX BRAS 关联特性

NE16EX 除了基本的 BRAS 功能外，还包括一些 BRAS 相关的特性：

- 支持动态路由器协议；
- 支持 L2TP、GRE、IPSEC、MPLS 等多种网络侧 VPN 技术；
- 支持网络侧 IPv6 功能；
- 支持 NAT 增强和防火墙；
- 支持 VRRP 协议，保证设备可靠性；
- 支持层次化 HQoS 调度；
- 支持 URL 过滤，过滤非法网站；
- 支持智能应用控制 SAC，内置 DPI，深度识别业务流量；
- 支持集成 OSP 单板，可基于 OSP 单板快速部署应用；

1.3.3 NE16EX 待支持 BRAS 功能

目前 NE16EX 作为 BRAS 还不支持部分特性，在后续的软件版本逐步完善。

- * 用户组管理；
- * 用户组播业务；

- * 多核分布式转发；
- * 双主控用户热备；
- * 支持层次化 Multi-play 调度；
- * 支持 IPv6 用户接入
- * 支持 BRAS 双机热备；

2 BRAS 基本功能

2.1 用户接入认证

2.1.1 认证技术概述

根据使用的介质，宽带接入通常包括使用电话线的 ADSL（Asymmetric Digital Subscriber Line）接入、使用五类双绞线的以太网接入、使用无线信号的 WLAN（Wireless Local Area Network）接入等。这些方式对用户来说，在物理上直观可见。但这些用户并不直接接入 BRAS 的端口，而是接入 DSLAM（Digital Subscriber Line Access Multiplexer）、LAN Switch、AP（Access Point）等接入设备的端口，然后接入设备再接入 BRAS 端口。因此用户的差异在接入设备上被屏蔽，BRAS 无需关心终端用户的接入方式，而是通过可见的终端用户到达 BRAS 的报文的协议栈来区分用户。并通过 PPP 认证、Web 认证、、802.1X 认证等方法与终端用户交互用户名和密码等信息，识别用户身份，为实现针对用户的控制和管理用户。除了对有线用户的功能，NE16EX 作为 WLAN AC 还支持对无线接入用户身份进行认证。

2.1.2 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，用户无需输入用户名和密码。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，路由器将增加该 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 服务器下发的策略来控制。

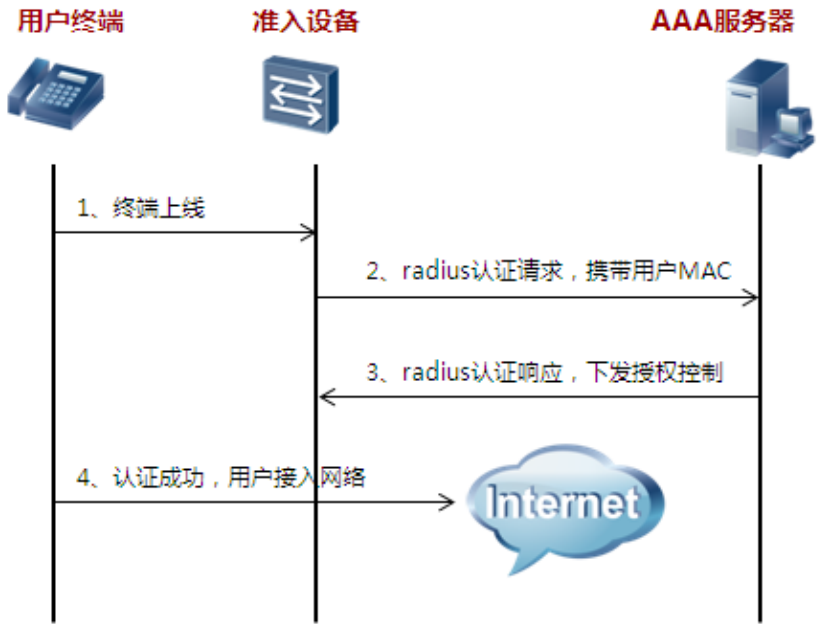

图2-1 MAC 认证流程图

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。

在 BRAS 路由器上，有线、无线用户均支持 MAC 认证接入。

2.1.3 802.1X 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，具体由 802.1X 客户端和 AAA 服务器协商确定。

- EAP-MD5（ Message Digest 5）

  EAP-MD5 使用 MD5 算法对用户密码和加密字（Challenge）生成消息摘要，到 AAA 服务器完成用户认证过程。由于需要输入用户名和口令，本方法容易受到字典攻击，但配置简单，广泛用于园区网络。

- EAP-PEAP（ Protected Extensible Authentication Protocol ）

  EAP-PEAP 主要指 EAP-MS-CHAPv2。服务器端需要提供证书，客户端使用用户名和密码进行用户身份验证。

- EAP-TLS（ Transport Layer Security ）

  EAP-TLS 使用了双向认证，客户端和服务器均拥有证书并进行相互间的身份证明。EAP-TLS 使用证书提高了安全性，但同时也意味着需要进行繁琐的证书管理。

- EAP-TTLS（ Tunneled Transport Layer Security ）

  EAP-TTLS 是 EAP-TLS 的增强版本，只需要服务器端证书。TLS 隧道建立后，采用用户名和密码进行认证。

下面以 EAP-MD5 为例，简要说明一下协议流程。

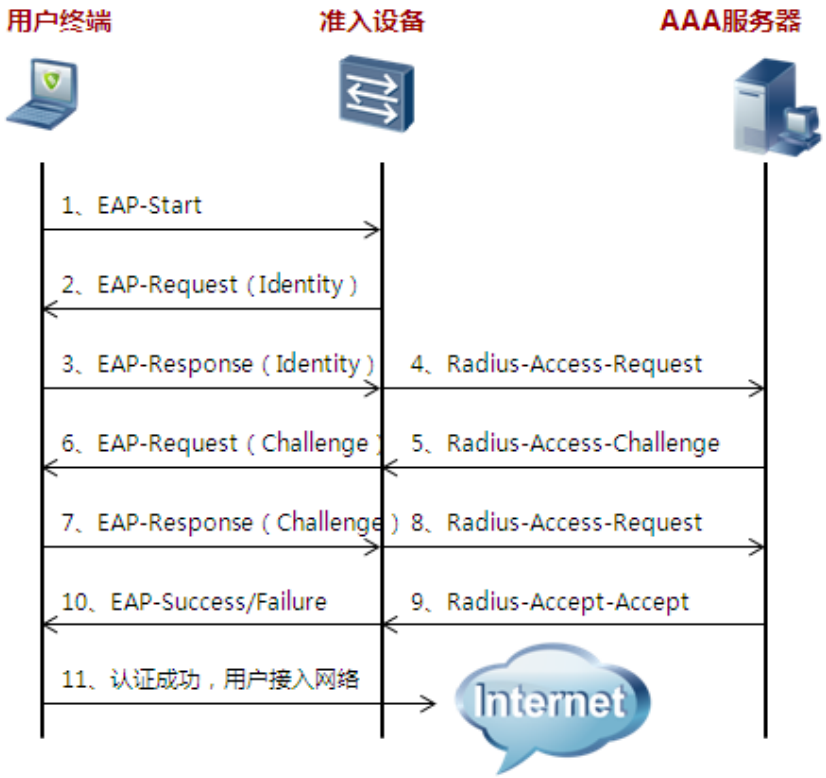

图2-2 802.1X EAP-MD5 认证流程图

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，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。

BRAS 路由器支持上述 802.1X 认证方式，可以做到基于客户端进行自适应不同 802.1X 认证机制。对于用户名方式认证，一般有线用户采用 EAP-MD5 方式，无线用户采用 EAP-PEAP 方式；对于基于证书的 802.1X 认证，可采用 EAP-TLS 方式。

2.1.4 Portal 认证

Portal 认证也称为 WEB 认证或 DHCP+WEB 认证。Portal 认证通过客户端或者标准 WEB 页面，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。

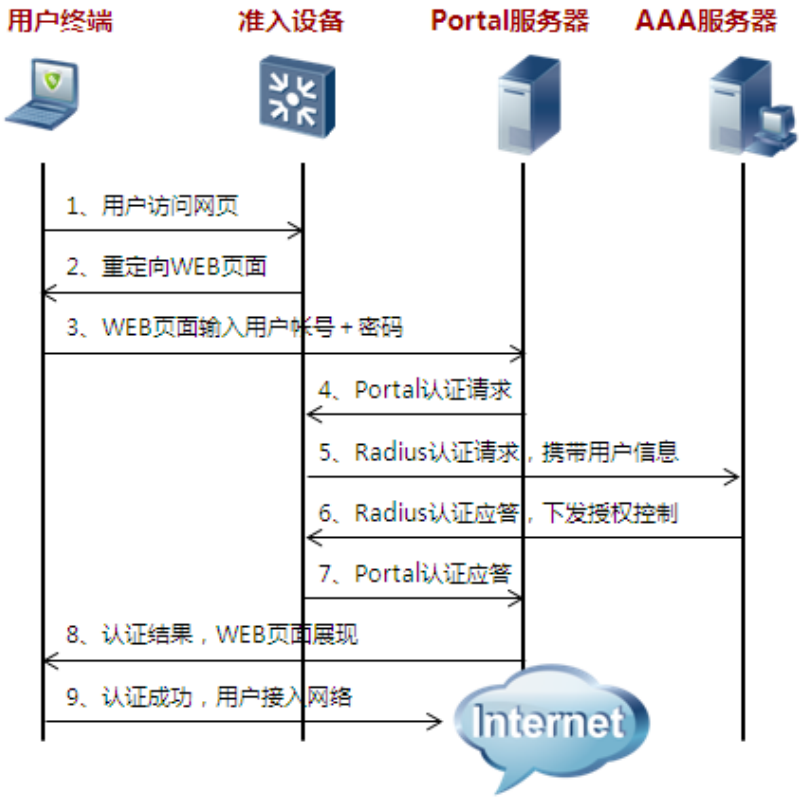

图2-3 Portal 认证流程图

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，此域名需要是 DNS 服务器可以解析的）。
2. 网络准入设备截获用户 HTTP 请求，如果请求报文目的地址不是 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。

在 BRAS 设备上，Portal 认证对于有线、无线用户均可以做到支持。

2.1.5 PPPoE 接入认证

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。

- PPPoE 发现阶段

  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。

- PPPoE 会话阶段

  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。

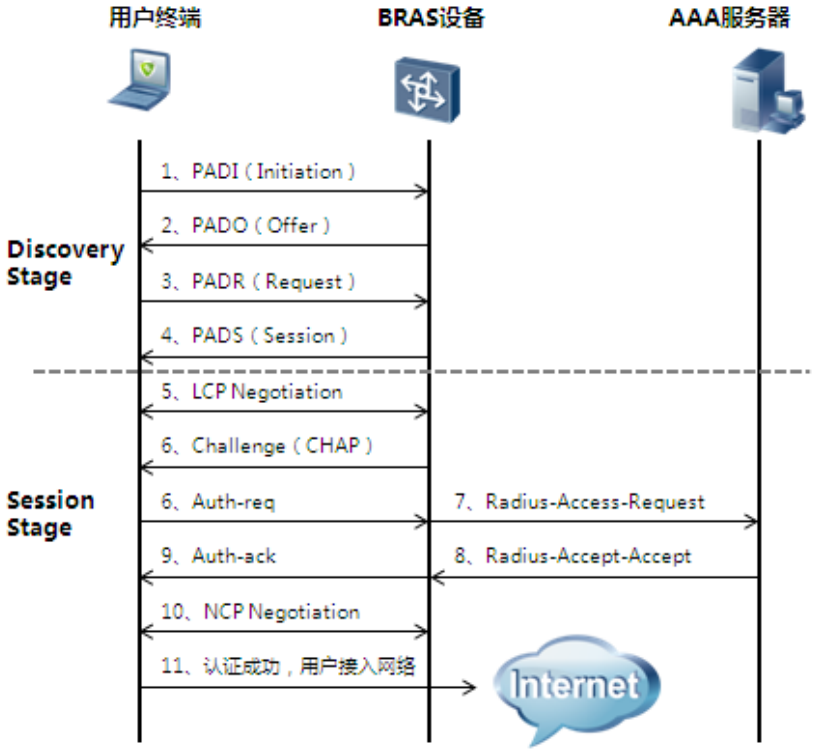

图2-4 PPPoE 认证流程图

详细的流程说明如下：

1. 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。
2. PPPoE 服务器向客户端发送 PADO 报文。
3. 客户端根据回应，发起 PADR 请求给 PPPoE 服务器。
4. PPPoE 服务器产生一个 Session id，通过 PADS 发给客户端。
5. 客户端和 PPPoE 服务器之间进行 PPP 的 LCP 协商，建立链路层通信。
6. 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。
7. 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。
8. 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。

9. PPPoE 服务器将认证结果返回给客户端。

10. 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。

11. 认证如果成功，用户则成功接入网络。

需要说明，PPPoE 认证仅对有线用户支持，无线用户不支持 PPPoE 认证。

2.1.6 L2TP 接入认证

L2TP（Layer 2 Tunneling Protocol，二层隧道协议）是 VPDN（Virtual Private Dial-up Network，虚拟私有拨号网）隧道协议的一种，是一种对 PPP 链路层数据包进行隧道传输的技术，允许二层链路端点（LAC）和 PPP 会话点（LNS）驻留在通过分组交换网络连接的不同设备上，从而扩展了 PPP 模型，使得 PPP 会话可以跨越 Internet 网络。

VPDN（Virtual Private Dial-up Network，虚拟私有拨号网）是指利用公共网络（如 ISDN 或 PSTN）的拨号功能接入公共网络，实现虚拟专用网，从而为企业、小型 ISP、移动办公人员等提供接入服务。即，VPDN 为远端用户与私有企业网之间提供了一种经济而有效的点到点连接方式。

L2TP 访问集中器（LAC，L2TP Access Concentrator）是交换网络上具有 PPP 和 L2TP 处理能力的设备。LAC 根据 PPP 报文中所携带的用户名或者域名信息，和 LNS 建立 L2TP 隧道连接，将 PPP 协商延展**错误！未找到引用源。**。LAC 可以建立不同的 L2TP 遂道使数据流之间相互隔离，即 LAC 可以建立多个 VPDN 连接。LAC 在 LNS 和 PPP 终端之间传递数据。即 LAC 收到 PPP 终端的报文后进行 L2TP 封装发送至 LNS，LAC 收到 LNS 的报文后进行解封装并发送至 PPP 终端。

L2TP 网络服务器（LNS，L2TP Network Server）是接收 PPP 会话的一端，通过 LNS 的认证，PPP 会话协商成功，远程用户可以访问企业总部的资源。对 L2TP 连接，LNS 是 LAC 的对端设备，即 LAC 和 LNS 建立了 L2TP 隧道；对 PPP，LNS 是 PPP 终端发起 PPP 会话的逻辑终止端点，即 PPP 终端和 LNS 建立了一条点到点的虚拟链路。LNS 位于企业总部私网与公网边界，通常是企业总部的网关设备。必要时，LNS 还兼有网络地址转换（NAT）功能，对企业总部网络内的私有 IP 地址与公共 IP 地址进行转换。

L2TP 典型组网图：

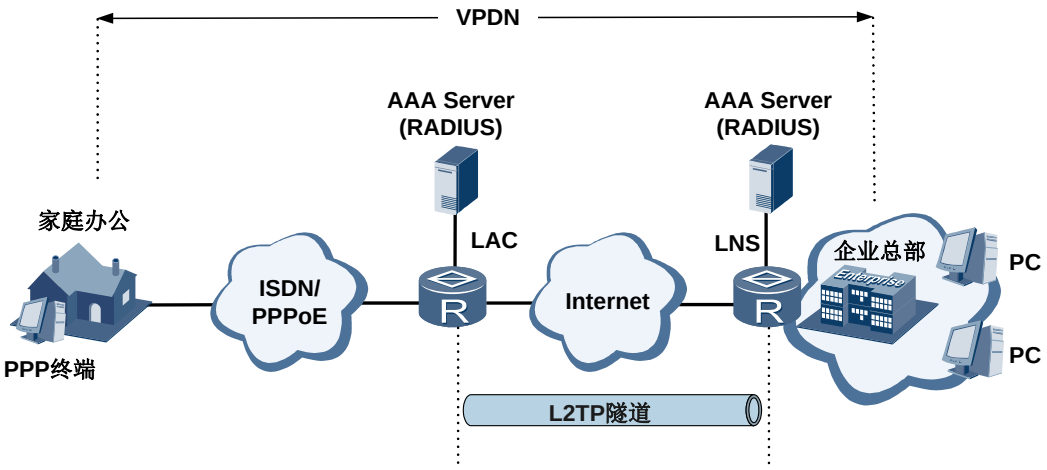

图2-5 L2TP 典型组网

进行隧道验证的 L2TP 隧道呼叫建立流程：

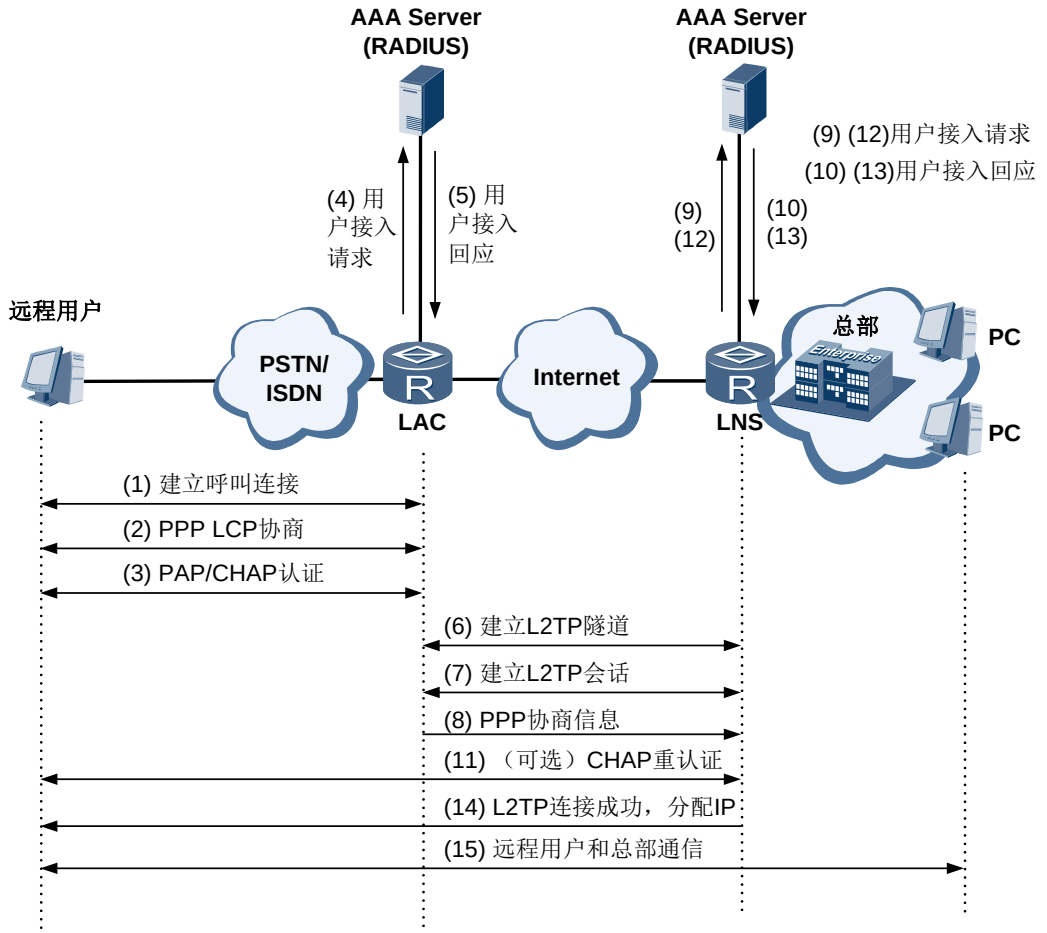

图2-6 L2TP 呼叫建立流程

接入认证流程：

1. 用户端 PC 机发起呼叫连接请求；

2. PC 机和 LAC 端进行 PPP LCP 协商；

3. LAC 对 PC 机提供的用户信息进行 PAP 或 CHAP 认证；

4. LAC 将认证信息（用户名、密码）发送给 RADIUS 服务器进行认证；

5. RADIUS 服务器认证该用户，如果认证通过，LAC 准备发起 Tunnel 连接请求；

6. LAC 端向指定 LNS 发起 Tunnel 连接请求；

7. 在需要对隧道进行认证的情况下，LAC 端向指定 LNS 发送 CHAP challenge 信息，LNS 回送该 challenge 响应消息 CHAP response，并发送 LNS 侧的 CHAP challenge，LAC 返回该 challenge 的响应消息 CHAP response；

8. 隧道验证通过；

9. LAC 端将用户 CHAP response、response identifier 和 PPP 协商参数传送给 LNS；

10. LNS 将接入请求信息发送给 RADIUS 服务器进行认证；

11. RADIUS 服务器认证该请求信息，如果认证通过则返回响应信息；

12. 若用户在 LNS 侧配置强制本端 CHAP 认证，则 LNS 对用户进行认证，发送 CHAP challenge，用户侧回应 CHAP response；

13. LNS 再次将接入请求信息发送给 RADIUS 服务器进行认证；

14. RADIUS 服务器认证该请求信息，如果认证通过则返回响应信息；

15. 验证通过，LNS 端会给远端用户分配一个企业网内部 IP 地址，用户即可以访问企业内部资源。

2.1.7 无线用户认证

无线接入和有线接入相比，由于无线报文在空口传输，报文可以被任何合适的接收设备捕获，所以无线用户不仅要进行认证，还要考虑无线空口的安全问题。

在无线用户接入过程中，BRAS 路由器作为有线无线一体化控制器（UC），具有 WLAN AC 功能。BRAS 路由器首先和接入设备 AP 建立 CAPWAP 管理隧道，管理所有下辖的 AP 设备；后续用户接入认证，BRAS 路由器和 AAA 服务器通过 RADIUS 协议进行。

图2-7 无线用户接入认证

参见上图，无线用户接入主要经过服务发现、链路认证、终端关联、接入认证、密钥协商、数据转发等六个阶段，其中前文提到的 MAC 认证、802.1X 认证、Portal 认证等技术，位于接入认证阶段，其他阶段都是无线用户上线独有的流程。

1. 服务发现

在无线领域中，用户终端也称为 STA（Station），STA 加入任何无线网络之前，必须先经过一番服务辨识的工作，称为 WLAN 服务发现过程。

WLAN AP 会主动发送 Beacon 帧通告提供的 SSID，STA 可以根据该报文确定周围存在的无线服务；STA 也可以指定 SSID 或者使用广播 SSID（即没有指定 SSID）主动地探测是否存在指定的无线网络，WLAN AP 接入端如果提供指定的无线服务，会发送确认信息给 STA。

服务发现成功后进入链路认证过程。

2. 链路认证

这是 STA 连入无线网络的起点，链路认证通过 Authentication 报文实现。

当前 802.11 的链路认证支持两种认证方式：开放系统认证（Open System Authentication）和共享密钥认证（Shared Key Authentication)。

3. 终端关联

一旦完成链路认证，STA 就可以跟 AP 进行连接，以便获得网络的完全访问权。

STA 客户端发起的 Association 或者 Re-association 请求，和 WLAN 服务端（包括 AP 和 AC）完成链路服务协商，建立了 802.11 链路。对于没有使能接入认证的 SSID，客户端已经可以访问无线网络；如果 WLAN 服务使能了接入认证，则 WLAN 服务端会发起对客户端的接入认证。

4. 接入认证

用户接入认证实现对接入用户的身份认证，为网络服务提供安全保护。对于无线用户接入认证，除了 MAC 认证、802.1X 认证、Portal 认证等方式外，还有无线特有的 PSK 认证。

在 802.11 链路协商的过程中，可以确定用户使用的接入认证算法（例如 EAP-PEAP），并且在链路协商成功后触发对用户的接入认证。

5. 密钥协商

密钥协商是数据加密传输的基础。密钥协商过程在逻辑上可以看作接入认证的一部分，只有在密钥协商成功以后，接入认证才会打开端口，允许用户的报文通过。

WLAN 密钥协商主要包括四次握手密钥协商和组密钥协商过程，这两种密钥协商都通过 EAPOL-Key 报文协商实现。WLAN 系统使用四次握手机制，进行单播数据报文使用的密钥协商；WLAN 服务端通过组密钥协商过程，将广播和组播使用的密钥通知所有的 STA 客户端。

6. 数据加密

接入用户身份确定并赋予访问权限后，网络必须保护用户所传送的数据不被窥视。数据的私密性通常是靠加密协议来达成的，只允许拥有密钥并经过授权的用户访问数据，确保数据在传输过程中的安全性。

2.2 AAA 和用户管理

2.2.1 AAA

2.2.1.1 概述

AAA 是 Authentication（认证）、Authorization（授权）和 Accounting（计费）的简称。

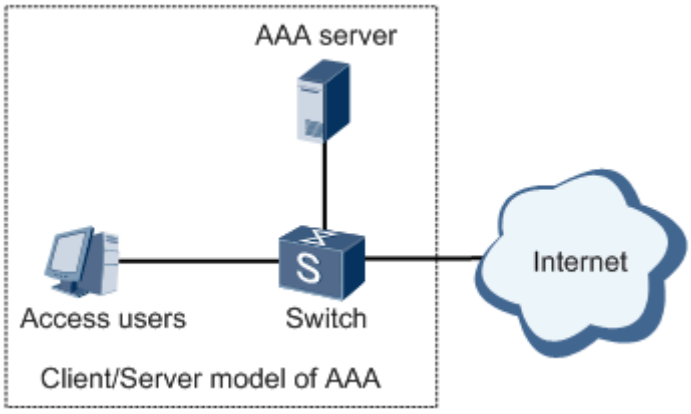

图2-8 AAA 基本架构示意图

它提供对用户进行认证、授权和计费三种功能。具体如下：

- 认证（Authentication）：验证用户是否可以获得访问权，确定哪些用户可以访问网络。
- 授权（Authorization）：授权用户可以使用哪些服务。
- 计费（Accounting）：记录用户使用网络资源的情况。

2.2.1.2 认证

AAA 支持以下认证方式：

- 不认证：对用户非常信任，不对其进行合法检查，一般情况下不采用这种方式。
- 本地认证：将用户信息配置在网络接入服务器上。本地认证的优点是速度快，可以为运营降低成本，缺点是存储信息量受设备硬件条件限制。
- 远端认证：将用户信息配置在认证服务器上。支持通过 RADIUS（Remote Authentication Dial In User Service）协议或 HWTACACS（HuaWei Terminal Access Controller Access Control System）协议进行远端认证。

2.2.1.3 授权

NE16EX 支持在用户上线过程中对用户进行授权，也支持用户在线情况下对用户进行动态授权。其中，在用户上线过程中，NE16EX 支持直接授权、本地授权、HWTACACS 授权、If-authenticated 授权等授权方案。

用户上线过程中授权：

- 本地授权：根据网络接入服务器为本地用户账号配置的相关属性进行授权。
- HWTACACS 授权：由 HWTACACS 服务器对用户进行授权。
- RADIUS 认证成功后授权：RADIUS 协议的认证和授权是绑定在一起的，不能单独使用 RADIUS 进行授权。
- if-authenticated 授权：适用于用户必须认证且认证过程与授权过程可分离的场景。即只有本地认证和 HWTACACS 认证支持该授权模式，RADIUS 认证不支持该授权模式。具体而言，
  - 本地认证成功后采用本地授权。
  - HWTCACS 认证成功后放开所有权限（免 HWTACACS 授权）。

NE16EX 使用用户域下的业务属性或 AAA 服务器下发的业务属性授权给用户。对于 AAA 服务器和用户域下都有的属性，域的业务属性比 AAA 服务器下发的业务属性优先级低，如带宽属性、流量控制属性等。当域的业务属性和 AAA 服务器针对用户下发的业务属性同时存在时，NE16EX 优先采用 AAA 服务器下发的业务属性。域的业务属性在 AAA 服务器不支持或者未下发该业务属性时生效。

用户在线授权：

NE16EX 支持用户在线情况下的动态授权。

动态授权是指用户在线情况下，在 AAA 服务器上重新设置 User-Group、CAR、Policyname 等属性值，AAA 服务器通过 CoA（Change of Authorization）报文下发给 AAA，AAA 动态更新用户的授权信息。有关 CoA 报文详细描述，请参见 RFC3576。

说明： 目前 NE16EX 仅支持通过 CoA 动态更新在线用户带宽。

2.2.1.4 计费

AAA 支持以下计费方式：

- 不计费：不对用户计费。

- 远端计费：支持通过 RADIUS 服务器或 HWTACACS 服务器进行远端计费。
- 实时计费：实时计费是指用户在线过程中，NE16EX 定时生成计费报文传送给远端计费服务器。实时计费是一种话单保护措施，目的是为了保证链路故障时能够最大程度地减少话单的误差，最大程度地保证计费信息的准确性。
- 计费失败策略：
  - 开始计费失败策略
    - 当开始计费失败时，如果失败处理策略是下线，则用户不能上线。
    - 如果失败策略是在线，则用户可以上线。
  - 实时计费失败策略
    - 当连续几次的实时计费请求都没有响应才会确认为实时计费失败时，如果失败处理策略是下线，则强制用户下线。
    - 如果失败处理策略是在线，则用户依然在线。

2.2.2 RADIUS 协议

远程认证拨号用户服务 RADIUS（Remote Authentication Dial-In User Service）是一种分布式的、客户端/服务器结构的信息交互协议，能保护网络不受未授权访问的干扰，常应用在既要求较高安全性、又允许远程用户访问的各种网络环境中。该协议定义了基于 UDP 的 RADIUS 帧格式及其消息传输机制，并规定 UDP 端口 1812、1813 分别作为认证、计费端口。

RADIUS 最初仅是针对拨号用户的 AAA 协议，后来随着用户接入方式的多样化发展，RADIUS 也适应多种用户接入方式，如以太网接入、ADSL 接入。它通过认证授权来提供接入服务，通过计费来收集、记录用户对网络资源的使用。

RADIUS 服务器：

RADIUS 服务器一般运行在中心计算机或工作站上，维护相关的用户认证和网络服务访问信息，负责接收用户连接请求并认证用户，然后给客户端返回所有需要的信息（如接受/拒绝认证请求）。

RADIUS 服务器通常要维护三个数据库：

- “Users”：用于存储用户信息（如用户名、口令以及使用的协议、IP 地址等配置信息）。
- “Clients”：用于存储 RADIUS 客户端的信息（如接入设备的共享密钥、IP 地址等）。
- “Dictionary”：用于存储 RADIUS 协议中的属性和属性值含义的信息。

RADIUS 客户端：

RADIUS 客户端一般位于网络接入服务器 NAS（Network Access Server）设备上，可以遍布整个网络，负责传输用户信息到指定的 RADIUS 服务器，然后根据从服务器返回的信息进行相应处理（如接受/拒绝用户接入）。

网络接入服务器作为 RADIUS 协议的客户端，实现以下功能：

- 标准 RADIUS 协议及扩充属性，包括 RFC2865、RFC2866。
- 华为扩展的私有属性。
- 对 RADIUS 服务器状态的主动探测功能。
- 计费结束报文的本地缓存重传功能。
- RADIUS 服务器的自动切换功能。

安全机制：

RADIUS 客户端和 RADIUS 服务器之间认证消息的交互是通过共享密钥的参与来完成的，并且共享密钥不能通过网络来传输，增强了信息交互的安全性。另外，为防止用户密码在不安全的网络上传递时被窃取，在传输过程中对密码进行了加密。

认证和计费消息流程：

RADIUS 客户端与服务器间的消息流程：

- 用户登录网络接入服务器时，会将用户名和密码发送给该网络接入服务器；
- 该网络接入服务器中的 RADIUS 客户端接收用户名和密码，并向 RADIUS 服务器发送认证请求；
- RADIUS 服务器接收到合法的请求后，完成认证，并把所需的用户授权信息返回给客户端；对于非法的请求，RADIUS 服务器返回认证失败的信息给客户端。

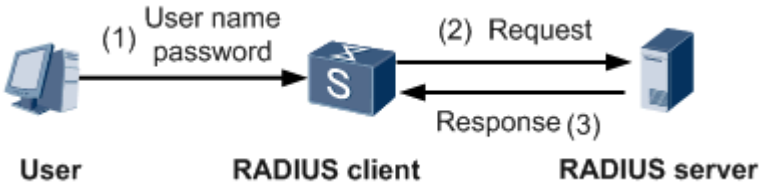

图2-9 RADIUS 客户端与服务器间的消息流程

计费的消息流程和认证/授权的消息流程类似。

2.2.3 HWTACACS 协议

HW 终端访问控制器控制系统协议 HWTACACS（Huawei Terminal Access Controller Access Control System）是在 TACACS（RFC 1492）基础上进行了功能增强的安全协议。该协议与 RADIUS 协议类似，采用客户端/服务器模式实现 NAS 与 HWTACACS 服务器之间的通信。

HWTACACS 协议主要用于点对点协议 PPP（Point-to-Point Protocol）和虚拟私有拨号网络 VPDN（Virtual Private Dial-up Network）接入用户及终端用户的认证、授权和计费。其典型应用是对需要登录到设备上进行操作的终端用户进行认证、授权、计费。设备作为 HWTACACS 的客户端，将用户名和密码发给 HWTACACS 服务器进行验证。用户验证通过并得到授权之后可以登录到设备上进行操作。

HWTACACS 协议和 RADIUS 协议的比较：

HWTACACS 协议与 RADIUS 协议都实现了认证、授权、计费的功能，它们有很多相似点：结构上都采用客户端/服务器模式；都使用公共密钥对传输的用户信息进行加密；都有较好的灵活性和可扩展性。

与 RADIUS 相比，HWTACACS 具有更加可靠的传输和加密特性，更加适合于安全控制。HWTACACS 协议与 RADIUS 协议的主要区别如表所示。

表2-1 HWTACACS 与 RADIUS 协议对比

HWTACACS	RADIUS
使用 TCP，网络传输更可靠	使用 UDP
除了标准的 HWTACACS 报文头，对报文主体全部进行加密	只是对认证报文中的密码字段进行加密
认证与授权分离	认证与授权一起处理
适于进行安全控制	适于进行计费
支持对设备上的配置命令进行授权使用	不支持

说明：

HWTACACS 协议与其他厂商支持的 TACACS+协议都实现了认证、授权、计费的功能。HWTACACS 和 TACACS+的认证流程与实现方式是一致的，HWTACACS 协议能够完全兼容 TACACS+协议。

2.2.4 用户管理

2.2.4.1 概述

对接入用户的管理是 BRAS 的主要职责。在目前的实现中，BRAS 对用户的管理分为两种方式：

- 通过域进行管理

  所有用户都属于一个域，缺省情况下，用户加入的是缺省域。通过在域下配置业务属性，对用户进行管理，同一个域下的用户具有相同的业务属性。

- 通过用户帐号进行管理

  是指在 RADIUS/HWTACACS 等 AAA 服务器上配置用户帐号及相应业务属性，在用户上线时下发给用户或者用户上线后动态下发。

在 NE16EX 的实际应用中，除了不认证以及不计费的应用之外，所有的用户帐号都配置在 AAA 服务器上，在 AAA 服务器上用户帐号的所有归属域都必须在 NE16EX 上进行对应的配置。NE16EX 支持本地用户帐号的配置和管理。

通常域的业务属性比 AAA 服务器下发的业务属性优先级低。当域的业务属性和 AAA 服务器针对用户下发的业务属性同时存在时，NE16EX 优先采用 AAA 服务器下发的业务属性。域的业务属性在 AAA 服务器不支持或者未下发该业务属性时生效。

2.2.4.2 域简介

NE16EX 中的用户名格式为“username@domain”或者“domain@username”，其中“@”为域名和用户名的分隔符。域名与用户名之间位置的先后关系可以配置，域名可以在前，也可以在后。如果用户在接入 NE16EX 时输入的用户名中不包含域名，则该用户属于系统的缺省域。

缺省情况下，设备存在配置名为 default 和 default_admin 两个域，全局默认普通域为 default，全局默认管理域为 default_admin。两个域均不能删除，只能修改。当无法确认接入用户的域时使用缺省域。

- default 用于接入用户（如 NAC）的缺省域，缺省为本地认证。
- default_admin 用于管理员（如 http，SSH，telnet，terminal，ftp）的缺省域，缺省为本地认证。

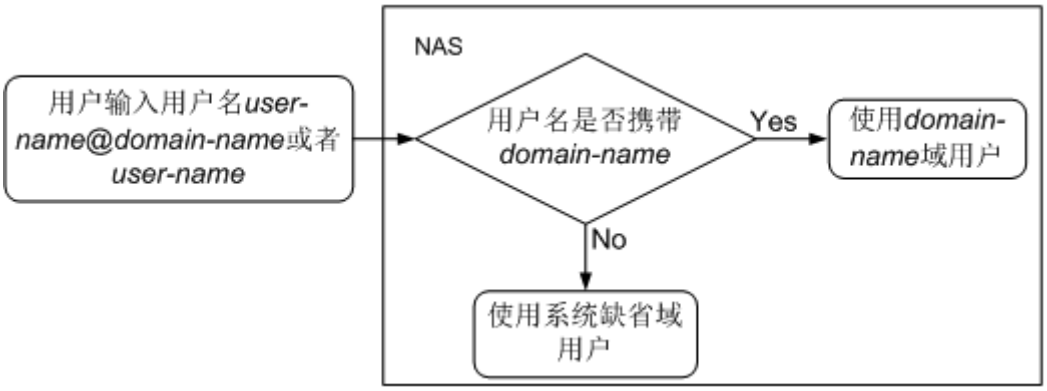

图2-10 用户名决定域

用户的认证、授权、计费都是在相应的域视图下应用预先配置的认证、授权、计费方案来实现的。AAA 有缺省的认证、授权、计费方案，分别为本地认证、本地授权、本地计费。如果用户所属的域下未应用任何认证、授权、计费方案，系统将使用缺省的认证、授权、计费方案。

2.2.4.3 域管理内容

域或 AAA 服务器通过配置用户的业务属性来管理用户，域管理的内容分为接入管理和业务管理两类。

接入管理：

通过域，可以指定用户接入使用的认证、计费、授权方案及相应的服务器，可以指定认证过程中使用的认证方式，可以指定为用户分配 IP 地址的地址池及 DNS 服务器。

业务管理：

用户上线后，可以通过域来管理用户使用接入业务权限、带宽、QoS 等。

- 强制 Portal

  强制 Portal，是指用户认证通过后第一次访问外部网络时，由 NE16EX 将其访问请求强制重定向到某一服务器（通常为运营商的 Portal 服务器），使用户访问 Internet 的第一站就是运营商站点的一项业务。

- 闲置切断功能

  闲置切断（Idle-Cut）是指当用户在某一个时长内业务流量小于某一个阈值时，NE16EX 认为该用户处于闲置状态，从而切断用户连接的功能。

- 流量统计功能

  流量统计功能包括域的总流量统计功能和用户的上下行流量统计功能。

- QOS 模板

  通过 QOS 模板配置用户的 QOS 属性。目前仅支持用户带宽控制。

- VPN 实例

  不同域下绑定不同 VPN 实例，不同域的用户属于不同的 VPN。

- 支持按剩余流量和剩余时长切断用户

  支持按剩余时长和剩余流量切断用户，支持剩余时长和剩余流量由 Radius 属性下发（需 Radius 服务器配套支持）。

2.3 地址分配与管理

NE16EX 具有完善的地址分配与管理机制，能为 IPv4 用户分配 IPv4 地址；地址分配方法既支持为用户动态的分配 IP 地址，也支持为用户配置固定的 IP 地址；同时能够通过地址池有效地管理 IPv4 地址。

2.3.1 地址分配技术

地址分配技术是指用户获取 IP 地址的方式，通常具有静态地址分配和动态地址分配两种方式。

- 静态地址分配

  是指用户自己在计算机上配置固定的 IP 地址，这种方式只适用于 IPoE 方式。

- 动态地址分配

  是指用户通过 IPCP（PPP 用户）、DHCP（IPoE 用户） 等协议，与 BRAS 设备交互后，由 BRAS 设备进行地址分配。在为 IPv4 用户分配 IP 地址时，BRAS 设备具备 DHCP Server 和 DHCP Relay 功能，能够从本地地址池和远端地址池中为用户分配 IP 地址。

2.3.1.1 静态地址分配

静态 IP 地址分配是用户在自己计算机上指定一个固定的 IP 地址，而管理员在设备上配置该 IP 地址属于合法的地址。这种方式一般用于服务器或有特殊需要的用户。

静态地址既可以从本地地址池分配，也可以从远端地址池分配。如果从远端地址池分配，BRAS 设备需要判断远端地址池中该 IP 地址是否空闲，如果空闲，则分配给用户，否则分配失败。如果从本地分配，需要先禁用地址，然后才能将禁用的地址分配给静态用户。

2.3.1.1 DHCP 地址分配

DHCP 是动态主机配置协议（Dynamic Host Configuration Protocol）的简称，是一种终端自动配置协议。它以 BOOTP（Bootstrap Protocol）协议为基础发展起来的，其作用是在 TCP/IP 网络中向用户主机提供配置信息。DHCP 采用客户端/服务器模式，由客户端向服务器提出配置申请，包括分配的 IP 地址、子网掩码、缺省网关等参数，服务器根据策略返回相应配置信息。

IPoE 用户一般通过 DHCP 协议进行动态地址分配，具有以下两种情况。

- 本地地址分配

  用户域下配置的地址池为本地地址池时，使用本地地址分配。此时 BRAS 设备通过内置的 DHCP Server 功能为用户进行本地地址分配。

- 远端地址池分配

  用户域下配置的地址池为远端地址池时，使用远端地址分配。此时 BRAS 设备通过 DHCP Relay 功能为用户从外部的 DHCP 服务器申请分配地址。

DHCP Relay 即 DHCP 中继，它实现了不同网段间的客户端和服务器之间的地址分配。DHCP Relay 承担 DHCP 客户端和服务器之间中继服务，将 DHCP 协议报文跨网段透传到目的 DHCP Server，最终使网络上的 DHCP 客户端可以共同使用一个 DHCP Server 进行地址分配。

客户端首次申请地址时通过 DHCP Relay 获得地址过程如下图所示。DHCP 客户端发送请求报文给 DHCP Server， DHCP Relay 收到该报文并适当处理后，以单播形式发送给指定的位于其它网段上的 DHCP 服务器。服务器根据请求报文中提供的必要信息，通过 DHCP Relay 将配置信息返回给客户端，完成对客户端的动态配置。

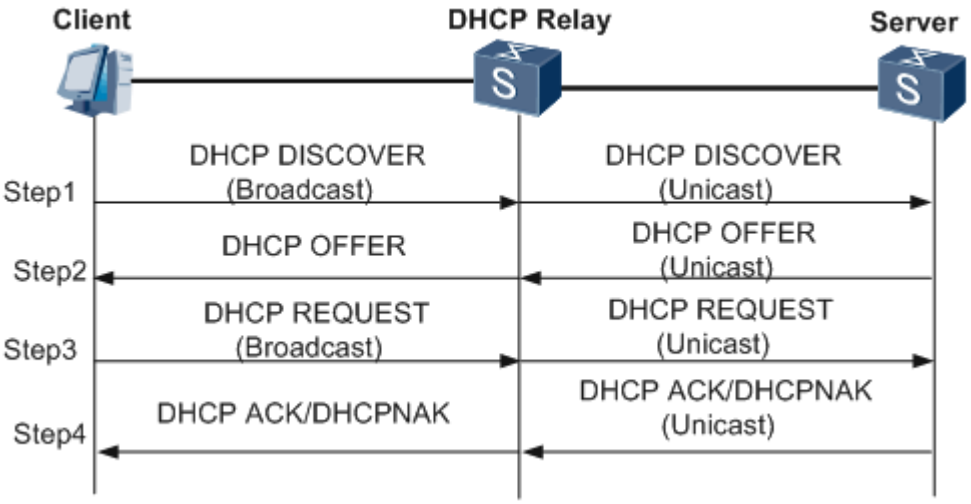

图2-11 DHCP Relay 地址分配流程

2.3.1.2 PPPoE 用户地址分配

PPPoE 用户的 IP 地址一般通过 PPP 协议簇中的 IPCP（Internet Protocol Control Protocol） 协议在 BRAS 设备中分配。IPCP 称为 IP 控制协议，此时 PPP 客户端可通过 IPCP 协商获取网段，网段的网关地址和网段的掩码须由 RADIUS 服务器下发。

PPP 用户可以使用三种方式获取 IP 地址：

- AAA 服务器认证成功后，通过认证响应消息给用户分配 IP 地址；
- AAA 服务器在认证成功的同时，给用户指定地址池号，由 BRAS 设备根据地址池进行远端地址分配或者本地地址分配。
- AAA 服务器认证成功后，BRAS 设备根据用户域下配置的地址池为其进行 IP 地址分配。

当使用本地地址池对 PPPoE 用户分配 IP 地址时，BRAS 设备需要查看地址池是否有空闲地址，如有，直接分配给用户。

2.3.2 地址管理技术

2.3.2.3 地址池

地址管理技术是指如何管理和组织所有用户的 IP 地址的技术，BRAS 设备通过地址池和地址前缀统一管理用户的 IP 地址。

- 本地地址池

  本地地址池是 BRAS 设备自行管理的地址池， BRAS 设备负责对地址池中的 IP 地址资源进行分配、续租、回收等管理。

- *远端地址池

  远端地址池是外部 DHCP/BOOTP 服务器的一个映像，里面并不配置实际的 IP 地址，只是指明该地址池对应的 DHCP/BOOTP 服务器。使用远端地址池时，BRAS 设备可以代理用户发起请求或者中继用户的请求，向 DHCP/BOOTP 服务器申请、续租或释放地址。

在地址池视图可配置 IP 地址池相关属性，包括地址范围、地址租期、网关地址、不参与自动分配的地址等信息。

2.3.2.4 地址池保护

当 IP 地址池中的一个或部分地址不能使用时，可以为该地址池设置保护，有四种方法：

- 锁定地址池

  地址池可以通过命令锁定，锁定后该地址池中的 IP 地址不再分配。本方法经常用于地址池由于有用户在线使用无法删除的情况，此时先锁定地址池，不再继续分配，待所有的用户下线后，地址池中的 IP 地址全部得到释放，再删除地址池。

- IP 地址禁用

  在复杂的网络规划中，可能需要对其中的部分 IP 地址进行禁用。

- IP 地址冲突标识

  当地址池中的 IP 地址与设备 IP 地址等冲突而无法使用时，可以通过该命令将相应的 IP 地址置为冲突，当冲突解除后，再手动解开。

- IP 地址回收

  当地址池中的 IP 地址出现异常时，即没有用户在使用，但 IP 地址处于被使用的状态，该 IP 地址无法被继续使用。此时可以通过 IP 地址强行回收命令进行回收。

2.3.2.5 地址池租期管理

BRAS 设备支持通过设置地址池租期来管理用户 IPv4 地址使用期限。当用户使用 IP 地址超过租期后，如果用户需要继续使用该地址，需要用户续租，续租是自动进行的，只要用户申请的 IP 地址合法可用，续租就会成功。地址租期管理分以下两种情况：

- 通过内置 DHCP Relay 功能分配的 IP 地址

  BRAS 设备转发外部 DHCP 客户端的地址续租请求报文，产生相应的续租请求消息，通过 DHCP Relay 功能，启动 IP 地址续租。

- 通过内置 DHCP Server 功能分配的 IP 地址

  BRAS 设备处理外部 DHCP 客户端的地址续租请求报文，为用户延长租期或者回收地址。

3 BRAS 业务应用

3.1 接入业务

3.1.1 普通用户接入

NE16EX 支持二层普通用户的接入。二层普通用户通过以太网（如用二层 LAN Switch）、ADSL（如用 DSLAM）、WLAN（如用 AP）等方式接入 NE16EX。

用户上网时，登录相应 WEB 页面（或者访问某个网页强制到 WEB 页面）输入用户名和密码后上网，还可以通过 PPP、802.1x 等拨号器拨号上网。

二层普通用户可以配置静态地址，也可以通过 IPCP、DHCP 协议由 NE16EX 负责分配和管理。二层普通用户拥有独立的业务属性，NE16EX 能够对其进行独立的认证、计费并对其业务进行控制和管理。

3.1.2 专线用户接入

NE16EX 支持三层专线用户接入。用户通过路由器等三层设备接入到 NE16EX 的某个接口或者接口的 VLAN。专线内用户的地址分配等工作由接入的三层设备负责，NE16EX 只作为转发路由器使用。NE16EX 可以通过 MAC 认证对下挂的三层设备进行合法性验证，专线上的各个终端用户的业务按专线的业务控制策略进行控制，流量全部采集在专线上，对专线统一作带宽限制。

PPPoE 专线与三层专线基本相同，也是通过路由器等三层设备接入到 NE16EX。在 PPPoE 专线方式下，三层设备作为 PPPoE Client，通过 PPPoE 拨号成为 NE16EX 的一个二层个人用户，因此在 NE16EX 上只能看到一个二层个人用户的存在，而看不到三层设备下的真实用户的存在。

3.1.3 强制 Portal 业务

NE16EX 支持强制 Portal 业务，从而使得运营商或企业可以通过 Portal 页面进行自我宣传，同时可以发布广告等业务。用户使用各种接入认证方式上网后，第一次访问外部网络时，NE16EX 将用户的 HTTP 请求强制重定向到指定的 Portal 页面，使得用户访问 Internet 的第一站就是强制 Portal 的页面。

3.2 增值业务

3.2.1 动态分配带宽

3.2.1.1 动态更改在线用户带宽

运营商想要管理在线用户带宽，例如在流量计费所包业务使用完毕自动降速，或者进行分时段对用户的带宽进行控制时，管理员可以在 RADIUS 服务器设置相应的计费策略。

用户按照某种接入认证方式上线，上线过程中获得基本的带宽。上线后，AAA 服务器根据该用户的计费策略，通过 Radius COA（Change of Authorization）协议给 NE16EX 下发用户的带宽。NE16EX 根据 AAA 服务器动态下发的带宽作为该用户的新带宽。

3.2.1.2 *用户按需选择带宽 BOD

随着 VoIP、IPTV 等网络应用的多样化，客户对网络带宽的需求也越来越多样化。BOD（Bandwidth On Demand）是为客户提供多样化服务的有效方案。

BoD 特性是一种针对用户实现动态分配带宽的增值业务，在用户有带宽调整需求时，可以通过 Portal 服务器自助选择 BoD 业务，业务动态激活和注销，不需要管理员通过更改配置，同时也给运营商提供了更为灵活的基于业务的计费方式。

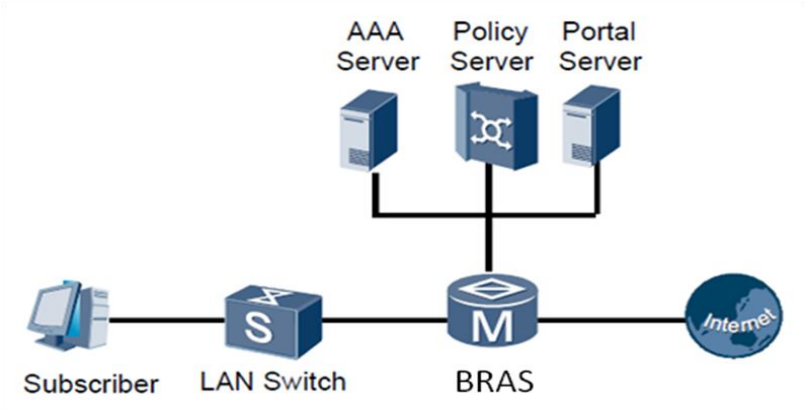

图3-1 BoD 业务组网

用户按照某种接入认证方式上线，上线过程中获得基本的带宽。上线后，用户访问 Portal 服务器，在 Portal 页面上选择自己需要的带宽类别，Portal 服务器把用户的选择提交给 Policy 服务器。Policy 服务器根据用户的选择，给 BRAS 下发用户的带宽索引。BRAS 根据带宽索引，从本地配置中获得具体的带宽数据，设置该用户的带宽。生效后，用户即可按照新的带宽使用网络。

BRAS 提供的 BOD 业务不仅可以动态分配带宽，也可以更改用户的 ACL 组、用户优先级、计费策略等一些基本用户属性。

3.2.2 目的地址计费

目的地址计费：DAA（Destination Address Accounting）实现了对用户接入业务的目的地址进行差异化管理，根据不同目的地址定义不同的费率级别进行收费。

以校园网为例：

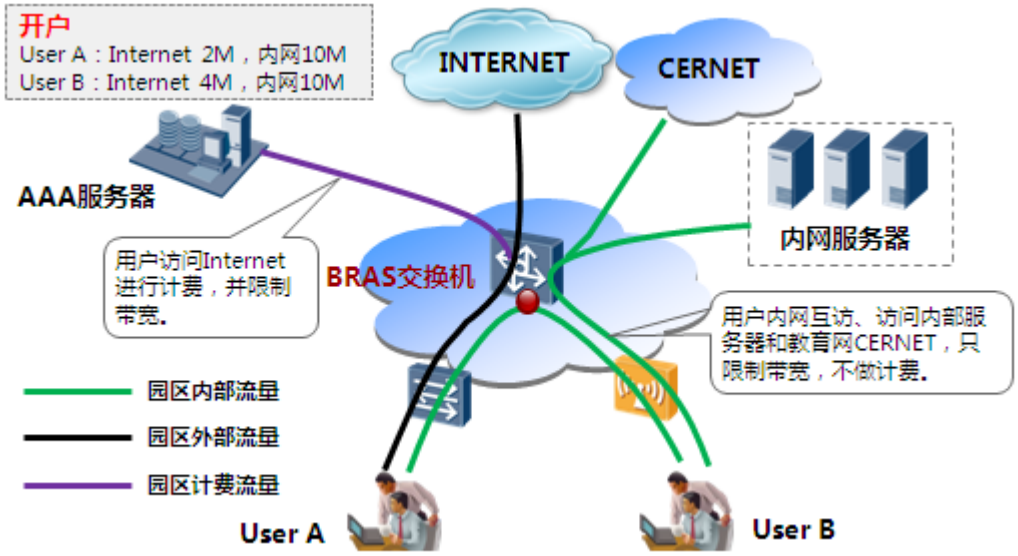

图3-2 DAA 实现差异化的带宽和计费策略

BRAS 路由器支持以下 DAA 功能：

- * 按目的地址实施带宽策略

  DAA 实现不同网络通道独立进行流量统计，将用户的内、外网流量区分开，可基于不同目的地址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 实现园区内网、外网分离控制的基础上，可实施不同的计费策略。例如，对于 User B，访问内部服务器和用户间互访流量不做计费，而访问 Internet 流量进行基于时间或者基于流量的费用计算。

说明：

目前 NE16EX 支持按目的地址实施计费策略。

3.2.3 深度报文分析 DPI

DPI（Deep Packet Inspection）是一种深度报文分析技术，能够将网络上的数据报文根据五元组分为一个个的应用流，并通过基于“特征字”的识别技术、应用层网关识别技术、行为模式识别技术等识别技术对应用流中的特定的数据报文进行探测，从而确定应用流对应的应用或者用户的动作。

NE16EX 上集成了 DPI 功能特性，能够识别并控制管理诸如 BT（BitTorrent）、eMule、eDonkey 等 P2P 业务报文，从而能够减少这些业务报文对网络造成的冲击和破坏，减少运营商的运营成本，提高运营商的服务质量。

3.2.4 非法网站 URL 过滤

在校园网等宽带接入场景，为防止学生对非法网站的访问控制，NE16EX 提供 URL 过滤功能，禁止用户访问一些非法网站或非法网站的内容，也保护学校内的计算机不受某些病毒的威胁。

NE16EX 支持本地 URL 过滤和远端 URL 过滤。本地 URL 过滤可以直接在设备上配置禁止访问的 ULR 地址。远端 URL 过滤需要到远端 URL 服务器查询 URL 分类信息和信誉度信息，根据返回的查询结果匹配相应的策略，根据策略中的动作执行相应的处理。由于远端 URL 分类信息后定期更新，可有效防止用户访问恶意网站。

3.3 *业务高可靠性

NE16EX 能够实现业务高可靠性技术，对接入业务进行设备间的备份，当主用设备的链路、接口、单板或者整机出现故障时，能够快速将业务切换至备用设备，业务中断时间不超过 200ms，当主用设备从故障中恢复后，业务能顺利由备用设备回切至主用设备且不会中断。

说明：

目前 NE16EX 不支持业务高可靠性。

4 产品规格

4.1 硬件规格

NE16EX 路由器可支持 BRAS 特性的单板包括：

- MSP40 主控板（Ethernet 接口：2*10GE、 4*GE COMBO）
- 4 端口-GE 光 WAN 接口卡
- 4 端口-GE 电 WAN 接口卡
- 4 端口-GE COMBO WAN 接口卡

4.2 功能规格

4.2.1 用户接入

- 支持 IPoE 用户接入
  - IPoE 用户类型： IPoE、IPoEoV；
  - 支持 DHCP Server、DHCP Relay 为用户分配 IP；
  - 支持 MAC 认证、802.1X 认证、强制 WEB 认证（Portal 认证）；
  - 支持 Web 认证用户根据 Vlan 推送指定的 Portal 页面；
- PPPoE 用户：
  - PPP 用户类型：包括 PPPoE、PPPoEoV、PPPoEoQ、PPPoLNS
  - 支持一个 MAC 多个 PPPoE 用户；
  - 支持限制一个 MAC 可以接入的 PPPoE 用户数；
  - 支持限制整机可以支持的 PPPoE 用户数；
  - 支持 CHAP 和 PAP 认证；

- 支持 PPPoE 用户的 VPDN 业务，将 PPPoE 用户续传到 LNS 终结；
- 支持 PPPoE Server 配置服务名称，根据服务名称限制用户接入；

- 支持同一接口同时接入 PPPoE 用户和 IPoE 用户
- 支持给 IPoE 用户或 PPPoE 用户强推 Portal 页面。

4.2.2 AAA

- 支持域管理：
  - 支持基于域的认证、计费、授权方案；
  - 支持域关联 radius 服务器或 hwtacacs 服务器
  - 支持域关联 IP 地址池、DNS 服务器、WINS 服务器
  - 支持域配置用户 QOS
  - 支持域配种用户 VPN
  - 支持域名解析规则配置
- 认证策略：
  - 支持不认证，本地认证，radius 认证，hwtacacs 认证，多次认证；
  - 支持 PAP、CHAP 认证
  - 支持管理用户，MAC 认证用户，802.1X 用户，WEB 用户，PPPoE 用户，LAC 和 LNS 用户认证
  - 支持 EAP 终结认证、EAP 透传认证
- 授权策略
  - 支持本地授权、radius 授权、hwtacacs 授权、if-authenticated 授权、多次授权；
  - 支持 RADIUS 服务器下发 COA 报文动态修改用户授权信息
  - 支持 RADIUS 服务器切断用户会话
  - 支持管理用户，MAC 认证用户，802.1X 用户，WEB 用户，PPPoE 用户，LAC 和 LNS 用户授权
- 计费策略
  - 支持不计费，radius 计费和 hwtacacs 计费；
  - 支持流量计费、时长计费、实时计费；
  - 支持计费失败策略配置，用户在线或下线；
  - 支持管理用户，MAC 认证用户，802.1X 用户，WEB 用户，PPPoE 用户和 LNS 用户计费

- 支持基于目的地址计费策略

4.2.3 RADIUS

- 认证
  - 支持标准 RADIUS 认证协议，RFC2865，RFC2869，RFC3579
  - 支持华为扩展 RADIUS 协议
  - 支持主备 RADIUS 认证服务器，支持对主服务器故障检测
  - 支持 EAP 透传
  - 支持 RADIUS 属性转换和 RADIUS 属性禁用
  - 支持 NAS IP 可配置
  - 支持 IPv6 认证服务器
- 授权
  - 支持标准 RADIUS 授权协议，RFC3576（动态授权）
  - 支持 RADIUS COA 功能
  - 支持 RADIUS DM 功能
- 计费
  - 支持标准 RADIUS 授权协议，RFC3576（动态授权）
  - 支持主备 RADIUS 计费服务器，支持对主服务器故障检测
  - 支持开始计费报文，停止计费报文和实时计费报文
  - 可配置计费报文中用户名属性是否携带域名
  - 计费报文携带用户信息和计费信息
  - 支持 IPv6 计费服务器

4.2.4 HWTACACS

- 认证
  - 支持 HWTACACS 协议
  - 支持主备 HWTACACS 服务器
  - HWTACACS 服务器源地址绑定配置

- 支持 IPv6 认证服务器

- 授权
  - 支持用户的 tacacs 授权
  - 命令行授权
  - 支持 HWTACACS 授权失败后跳转本地授权
- 计费
  - 计费报文中用户名中是否携带域名
  - 支持开始计费报文，停止计费报文和实时计费报文
  - 支持按时长计费
  - 支持 IPv6 计费服务器

4.2.5 地址管理

- 支持从本地地址池为用户分配地址
- 支持配置地址池网关和地址段范围
- 支持配置 DNS 服务器和 NetBIOS 服务器
- 支持地址池绑定 VPN 实例
- 支持用户 MAC 地址和 IP 绑定
- 支持去除不能为用户分配的地址
- 支持 RADIUS 下发 PPP 用户的 IP 地址、或指定地址池；

4.2.6 L2TP

- LAC
  - 支持 LAC 根据 PPPoE 用户的用户名或域名来判断是否是 VPDN 用户
  - 支持主备 LNS 功能
  - 支持 AVP 数据隐藏
- LNS
  - 支持与远端 PPP 用户进行强制 LCP 重协商
  - 支持对远端 PPP 用户进行强制 CHAP 认证

- 支持远端用户接入到公司内部网络的 VPN
- 支持通过 RADIUS 服务器分配 IP 地址给 L2TP 用户
- 支持处理 RADIUS 下发的分支机构路由
- 支持 AVP 数据隐藏

4.3 License

- 通过 License 控制 PPPoE 用户数
- PPPoE 用户数初始为 1K，每个 License 增加 1K

参考标准

表4-1 BRAS 特性标准跟踪表

文档	描述	备注
RFC 2903	Generic AAA Architecture	
RFC 2904	AAA Authorization Framework	
RFC 2905	AAA Authorization Application Examples	
RFC 2906	AAA Authorization Requirements	
RFC 2989	Criteria for Evaluating AAA Protocols for Network Access	
RFC 3539	Authentication, Authorization and Accounting (AAA)	
RFC 2809	Implementation of L2TP Compulsory Tunneling via RADIUS	
RFC 2865	Remote Authentication Dial In User Service (RADIUS) (June 2000)	
RFC 2866	RADIUS Accounting (June 2000)	
RFC 2867	RADIUS Accounting Modifications for Tunnel Protocol Support	
RFC 2868	RADIUS Attributes for Tunnel Protocol Support	
RFC 2869	RADIUS Extensions (June 2000)	
RFC 2882	Network Access Servers Requirements: Extended RADIUS Practices	

RFC 3162	RADIUS and IPv6	
RFC 4818	RADIUS Delegated-IPv6-Prefix Attribute	
RFC 3575	IANA Considerations for RADIUS (Remote Authentication Dial In User Service)	
RFC 3579	RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)	
RFC 3580	IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines	
RFC 4014	Remote Authentication Dial-In User Service (RADIUS) Attributes Sub option for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option	
RFC 0927	TACACS user identification Telnet option	
RFC 1492	An Access Control Protocol, Sometimes Called TACACS (July 1993)	

术语与缩略语

术语与缩略语	英文全名	中文全称
AAA	Authentication Authorization Accounting	认证、授权、计费
BRAS	Broadband Remote Access Server	宽带远端接入服务器
RADIUS	Remote Authentication Dial In User Service	远端接入用户服务器
SVF	Super Virtual Fabric	超级虚拟交换网
ENP	Ethernet Network Processor	以太网络处理器
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DHCPv6	Dynamic Host Configuration Protocol for IPv6	DHCPv6 协议
ARP	Address Resolution Protocol	地址解析协议
ND	Neighbor Discovery	ND 协议
PAP	Password Authentication Protocol	密码验证协议
CHAP	Challenge Handshake Authentication Protocol	质询握手验证协议
WLAN	Wireless Local Area Network	无线局域网
CAPWAP	Control and Provisioning of Wireless Access Points	无线接入点控制协议
UC	Unified Controller	有线无线一体化控制器
CUC	Center Unified Controller	集中式一体化控制器
AC	Access Controller	WLAN 接入控制器
AP	Access Point	WLAN 无线接入点

术语与缩略语	英文全名	中文全称
AS	Access Switch	接入交换机
SSID	service set identifier	服务器标识
PSK	Pre-shared key	预共享密钥认证
WEP	Wired Equivalent Privacy	有线等效保密
WPA/WPA2	Wi-Fi Protected Access	Wi-Fi 安全访问协议
TKIP	Temporal Key Integrity Protocol	临时密钥完整性协议
CCMP	Counter Mode with CBC-MAC Protocol	计数器模式及密码块链消息认证码协议
WAPI	WLAN Authentication and Privacy Infrastructure	无线局域网鉴别和保密基础结构
WAI	WLAN Authentication Infrastructure	无线局域网认证基础结构
WPI	WLAN Privacy Infrastructure	无线局域网保密基础结构
BoD	Bandwidth On Demand	按需分配带宽
DAA	Destination Address Accounting	按照目的地址计费
COPS	Common Open Policy Service Protocol	通用开放策略服务协议
CSS	Cluster Switch System	集群交换系统
HQoS	Hierarchical Quality of Service	服务质量
FQ	Flow Queue	流队列
SQ	Subscriber Queue	用户队列
GQ	Group Queue	用户组队列
CQ	Class Queue	类队列
PQ	Port Queue	端口队列
TCO	Total Cost of Ownership	总体拥有成本
CERNET	China Education and Research Network	中国教育和科研计算机网
CNGI	China Next Generation Internet	中国下一代互连网