联营网吧管理关键技术及开发方案

Co-net-bar Management Key Technology and Application Design

摘　要：本文对宽带IP网发展过程中产生的三种授权认证计费关键技术(Authorize, Authenticate and Account 简称AAA)进行分析、比较，提出了对联营网吧认证授权计费监控管理系统的设计方案。

关键词：联营网吧　授权　认证　计费

王素贞（河北经贸大学计算机与网络中心　050091）
杨　洁（石家庄中国网通石家庄分公司　050091）

目前，宽带IP网络的应用正处于起步阶段，“联营网吧”是运营商和经营商采用的主要商业运作模式之一。由于宽带IP网具有巨大的潜在应用市场，所以“联通”、“铁通”、“网通”都相继出台了对“网吧”接入专线的“包月制”优惠政策。这样做有两个问题解决不好，一是：收费方式单一,不能体现多用多收费，少用少收费的公平收费原则。二是：不方便收取新的增值业务费用(如：PC-to-Phone、发送短信等业务)。采用灵活、准确的授权认证计费管理系统，既是提高用户数量和扩大用户用网规模的关键，也是运营商和经营商赢利的关键。本文在对宽带IP网建设与发展过程中产生的三种认证与计费的前沿核心技术进行分析、比较研究的基础上，提出对联营网吧认证、授权、计费、监控管理系统的开发设计方案。

1 宽带IP城域网结构及接入

宽带IP城域网的网络结构可分为四层：核心层、汇聚层、小区层和楼宇层。核心层和汇聚层泛指为城域网的骨干，其建设由运营商负责组建。小区层和楼宇层泛指接入网，其建设可以由运营商，也可以由其他机构负责组建。考虑到网络的扩展性和稳定性，在网络骨干中一般采用路由技术，而交换只发生在接入部分，用户的以太网数据流在网络汇聚层转变为路由方式进行传送。在设备的选型上，骨干路由设备主要为路由器和高端的路由交换机，接入网的设备主要为ADSL、Modem、DSLAM和二层以太网交换机。本文主要讨论运营商对联营网吧接入管理的核心技术及设计方案。接入部分示意图如图1所示。

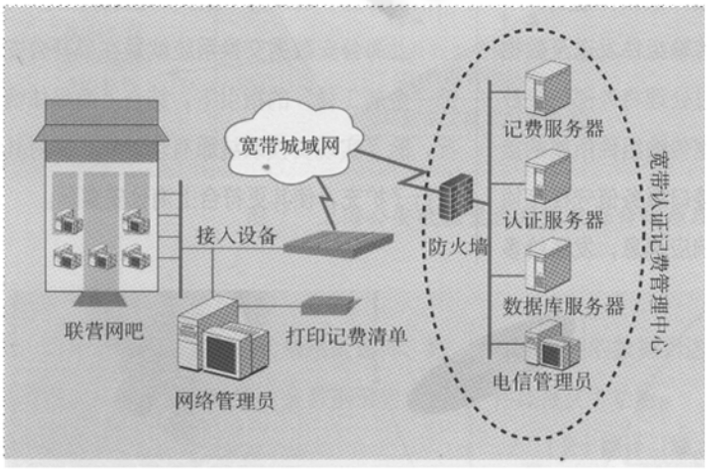

图 1　宽带 IP 城域网接入部分示意图

2 用户管理核心技术

网络运营的技术基础是网络用户管理技术，即对用户进行授权、认证、计费，简称AAA（Authorize，Authenticate，Account）技术。目前AAA的前沿技术主要有三种，分别是PPPoE方式、Web方式、802.1x方式，下面对这三种认证方式加以分析与比较。

2.1 三种技术优缺点及其比较

2.1.1 PPPoE方式

即以太网上的点对点协议（PPP over Ethernet）技术，主要目的是把最经济的局域网技术、以太网和点对点协议的可扩展性及管理控制功能结合在一起。它使服务提供商在通过数字用户线、Cable Modem或无线连接等方式，提供多用户的宽带接入服务时更加简便易行。PPPoE认证的优点是：它是窄带拨号技术在以太网接入技术的延伸，和原有的窄带网络用户接入认证体系一致，最终用户比较容易接受。并且业界的设备大部分都支持。缺点：由于PPPoE的网络直路本质，宽带接入服务器可能会成为网络的“瓶颈”，而且PPP协议需要再次封装，封装的效率很低。PPPoE的发现阶段会产生大量的广播包，影响网络的性能，需要有专门的客户端软件进行登录。

2.1.2 Web方式

Web认证技术是用户使用Web方式，通过在浏览的页面中输入用户名和密码实现对用户的认证。Web认证是目前比较流行的认证方

式。它不需要特殊的客户端软件，与系统平台无关，使用DHCP得到IP地址，没有额外的封装开销，并支持多播协议。但Web认证承载在七层协议之上，对于设备的要求较高，建网的成本高，用户的连接性差，不容易检测到用户离线。

2.1.3 802.1x认证

IEEE802.1x是基于端口的访问控制协议，能够在利用IEEE802局域网的优势基础上，提供一种对连接到局域网设备或用户进行认证和授权的手段。通过这种方式的认证，能够在局域网这种多点访问环境中提供一种点对点的识别用户的方式。802.1x协议为二层协议，不需要到达三层，且接入层的交换机不需要支持802.1q，业务报文直接承载在二层报文上，用户通过认证后，业务流和认证流分离，对后继的数据包没有特殊要求。但是该协议目前还没有正式的标准化，与802.1q不兼容，而且也需要专门的客户端软件进行登录。

2.1.4 三种技术比较

从以上多个角度的分析，各种方式各有优缺点。关于这三种方式的普及率，以PPPoE为最多；Web方式正得到越来越多的设备厂商的支持，它将更加受运营商的青睐；而802.1x为新的技术，只有少量厂家支持。基于PPPoE的认证方式，可管理性强，计费准确，代价就是PPP本身限制了网络环境以及组播业务的开展。不过国际上为了解决这个问题，近来提出了一些草案（IPmulticasting and broadcasting extension for PPPoEProtocol），尝试解决PPPoE上的组播问题。如果是运营商偏重系统的管理性、计费的精确性，建议采用PPPoE的认证计费技术。

2.2 基于 PPPoE 方式管理系统的特点

目前，就认证技术的成熟度来讲，以PPPoE方式为最高。基于PPPoE 方式的管理系统有以下应用特点：

2.2.1计费的准确性

对于PPPoE方式，在用户认证通过后，由宽带接入服务器BAS，向后台的RADIUS服务器发送计费开始包，在用户下线后（用户主动挂断、异常死机、网络断等），由BAS向后台的RADIUS服务器发送计费结束包。后台计费系统便可根据计费起始包、结束包按时长、按流量进行实时计费。以这种方式，计费数据相当准确。

2.2.2 对网络环境的要求

PPPoE的本质就是在以太网上运行PPP协议。由于PPP协议认证过程的第一阶段是Discovery阶段，广播只能在二层发现BAS。因此，也就决定了在用户主机和BAS之间，不能有路由器或三层交换机。另外，由于PPPoE的点对点的本质，在用户主机和BAS之间，限制了组播协议的存在。这将会在一定程度上，影响今后视频业务的开展。

2.2.3 可管理性强

对于PPPoE方式，宽带接入服务器与RADIUS服务器配合，可以进行一定程度的服务质量控制。很多的接入服务器都能够实现Policing和rate-limiting等功能。Policing是一种接收控制功能，只容许指定速率的流量通过。类似地，rate-limiting是发送控制功能，只容许指定速率的流量发送。

2.2.4 IP地址分配

PPPoE方式下的IP地址分配，完全是由宽带接入服务器和RADIUS服务器配合完成，用户不能修改。同时，后台的支撑系统还能够根据不同的用户分配不同范围、不同性质的IP地址，如某些用户使用公网地址，某些用户使用私有地址。

2.2.5 客户端软件限制

使用PPPoE进行用户认证，必须在客户端安装虚拟拨号软件。通过此虚拟拨号软件来与运营商局端的宽带接入服务器来完成PPPoE的连接。但随着WindowsXP的发布，微软已把PPPoE虚拟拨号的功能集成到操作系统中。

2.2.6 多服务选择能力

在宽带环境下，需要给不同用户提供不同服务的选择。在PPPoE方式下，许多厂家的宽带接入服务器提供类似“虚设备”的处理模块，不同的用户能够基于不同的“虚设备”，而引导至不同的服务区域。在国内电信环境下，大多数国内外主流的宽带接入服务器，都支持PPPoE接入。

3 系统方案设计

3.1 主要设备连接

系统主要设备有（1）路由器；（2）Radius系列服务器(数据库服务器、认证服务器、计费服务器)；（3）网吧终端机；（4）防火墙（Fire Wall）等。系统主要设备连接如图2所示。

3.2 系统工作原理

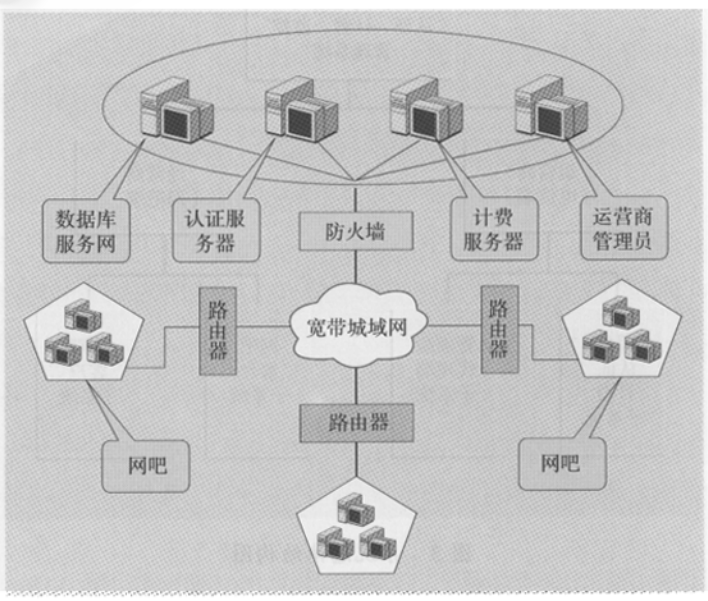

图2 系统主要设备连接示意图

系统在数据链路层通过PPPoE拨号对网吧里要接入的用户终端进行认证，对已通过认证的用户，在IP层对该用户进行计费。由路由器完成验证报送、控制、数据采集工作；用Radius服务器上的认证计费软件、接入管理软件作为后台处理软件,完成开户、计费、收费、统计等工作。利用路由器及RADIUS服务器系列提供的控制功能，运营商端可以有选择地对经营商端用户实施流量、宽带、时长、时段、功能、服务范围、服务质量、强制中断等控制；用户的注册信息放在数据库服务器上；当终端用户登录时，认证服务器对其进行认证，只许合法用户登录；登录成功后，计费服务器进行计费，计费的核心包括预定的服务类型、服务质量、统计数量、时长、次数等。AAA（授权、认证、计费）服务器与Internet之间必须使用防火墙隔离以保证其安全性。

3.3 系统总体结构

在进行总体结构设计时着重考虑了以下两点：其一，由于运营商和经营商是一对多的关系，即运营商下属的联营网吧少则几百家，多则上千家，为了方便运营商的管理，本系统设置了代理商管理功能，使经营商可以方便地委托其代理商进行代理管理。其二，记费子系统是本系统的核心，其中一部分功能放在管理端，便于统计某一联营网吧或所有联营网吧的营业额，监控其收支状况。另一部分功能放在吧台端，便于吧台日常经营时的管理与核算。基于以上考虑，逻辑上把本系统划分为四个子系统，分别是：授权认证记费子系统、管理端和代理端子系统、网吧前台子系统、网吧客户端子系统。其中，授权认证记费子系统和管理端和代理端子系统放在电信端，而网吧前台子系统和网吧客户端子系统放在网吧端。系统结构如图3所示。

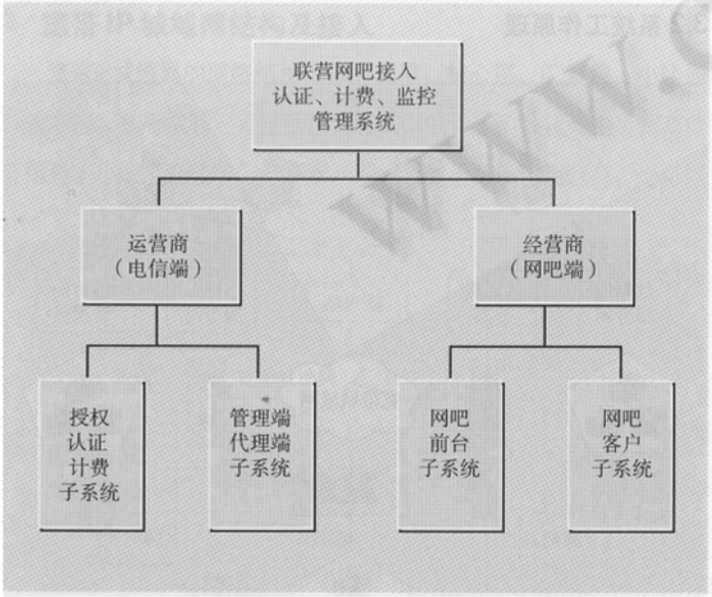

图 3　系统总体结构图

3.4 各个子系统的功能

3.4.1 认证记费子系统的主要功能

（1）授权（Authorize）由管理和代理子系统配合完成对联营连锁网吧的授权，使之合法。

（2）认证（Authenticate）对网吧内客户端的开通进行认证。若合法则开通，否则拒绝。

（3）记费（Account）记录网吧内已通过认证的客户端的以下信息：网吧标识、机器编号、开机时间(年-月-日 时:分:秒)、单价、消费时长、实收金额、上行流量、下行流量。

3.4.2 管理端代理端子系统的主要功能

（1）网吧管理：添加、删除、修改、查询联营连锁网吧的信息(多种查询方式)。

（2）记费管理：记费组合查询； 计费历史查询。

（3）统计分析：综合统计；按收入排序统计；按时长排序统计；按流量排序统计。

（4）管理员设置：添加管理员；删除管理员；修改管理员资料。

（5）状态监控：网吧状态监控；单机状态监控。

（6）发送消息： 向代理商发送消息；向网吧发送消息。

（7）代理商管理：添加、删除、修改、查询代理商。

3.4.3 网吧前台子系统的主要功能

（1）记费系统：开机；结帐；消息通知；监控；调换机器

（2）会员管理：新增会员；会员资料修改；添加费用。

（3）当前状态信息：当前状态信息功能提供了多种状态信息的查询方式。

（4）记费统计记录：提供多种方式营业记录。

（5）系统设置：记录设置（收费历史记录、操作历史记录、网站历史记录）；密码设置；记费标准设置（上网费率、会员记费）；管理员设置。

3.4.4 吧客户端子系统的主要功能

（1）新建模块：资源添加模块、用户菜单管理模块。

（2）管理模块：密码管理、安全管理、启动管理、外壳管理、限制模块、禁止模块。

（3）记录模块：单机详细记录、历史记录。

（4）网站模块：网站历史记录、网站限制。

3.5 各个子系统之间的信息存储与交换

联营网吧客户端产生的上网数据由网吧前台汇集起来上传到计费服务器；管理端可以实时查询、监控授权认证数据库、计费数据库，同时，管理端可以给网吧前台下传各种管理消息。各个子系统之间数据传输和信息交换如图4所示。

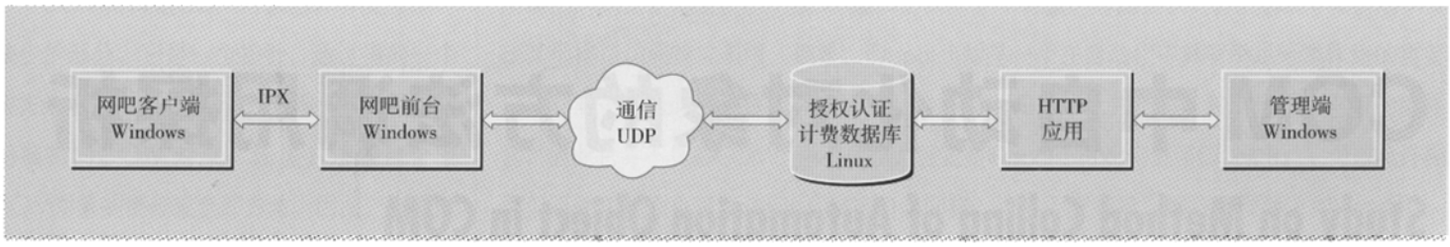

图4　子系统之间信息交换

4 系统实现

4.1 系统所用协议

管理端和代理端子系统与认证记费子系统之间采用HTTP协议实现；认证记费子系统与网吧前台子系统之间采用UDP协议实现；网吧前台子系统与网吧客户端子系统之间采用IPX协议实现。管理端和代理端子系统、网吧前台子系统与网吧客户端子系统均采用操作系统windows98/windows2000；认证记费子系统采用Linux操作系统。认证服务器与Internet之间使用防火墙进行安全隔离。

4.2 系统数据处理流程

当网吧吧台端有客户申请开机上网，系统即开始认证，通过认证后，系统授权开机，计费服务器开始计费。同时，管理端对该营业网吧和该客户机可以实施管理与监控。整个系统数据处理流程如图5所示。

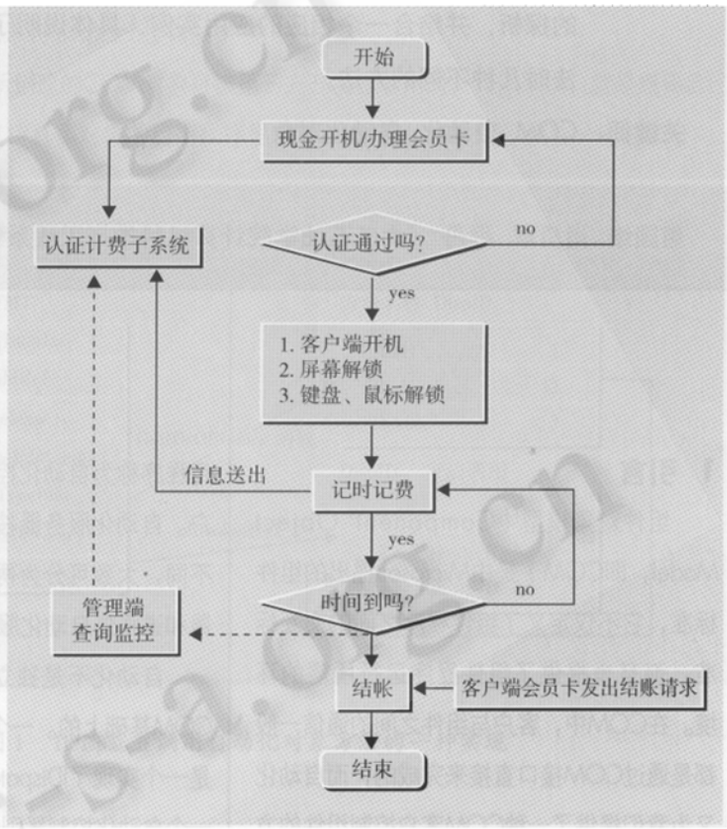

图5　系统数据处理流程图

参考文献

1 杜宾，宽带城域网的建设与以太网的发展，网络世界，第8期，2002.3。

2 钟健松，宽带网认证计费方式比较，北京朗新信息系统有限公司，2002.10。

3 罗娟，网络计费系统的关键技术，网络世界，第27期，2002。

4 段宁华，网络应用解决方案，人民邮电出版社，2001。