使用 IC 卡管理 Internet 开放实验室

邓劲生　赵振宇　张银福　（长沙　国防科大计算机学院　410073）

摘要：本文以 IC 卡应用系统为基础，介绍了使用 IC 卡管理 Internet 开放实验室的策略，并给出设计实现方案。

关键词：IC 卡　Internet　实验室

一、IC 卡应用系统

一般的 IC 卡应用系统中，管理主机负责有关应用信息的集中、处理、存储、显示和打印等，通过接口设备进行读写等信息交互工作。用户可通过键盘输入个人密码使用系统，通过主机显示屏查看数据及操作提示信息。主机可用通用 PC 机、工作站或高档服务器等，连接带小键盘的 IC 卡读写器。

为了避免外单位的 IC 卡在本单位系统使用，卡的发行区在写入发行部门代号后进行熔断操作，使发行代码不可更改。卡的写入密码由 IC 卡管理员掌握并严格保密，通常使用作向卡中存钱或更改个人密码用。个人区存放合法持有人的用户 ID 等具有唯一性的个人识别信息。如有必要，可将用户数据如剩余金额等加密后再存入卡中，以防止他人读出数据或非法复制卡片。

各学校现有开放机房往往采用现金购买机时票据，收票上机的方式，只能定时开放定量收款，造成管理松懈和上机不便。对于 Internet 开放实验室，由于用户上机时间长度和上网数据流量往往不确定，使用 IC 卡是必然选择。

二、系统设计方案

Internet 开放实验室的建设主要分为服务器和客户机两大部分。根据上述问题和安全考虑，将实验室建成为一个基于代理的 Intranet 方案比较可行。系统采用客户/服务工作模式，服务器有代理服务器、数据库服务器、IC 卡服务器等，一般运行 Windows NT Server。客户机可采用多种操作系统如 Windows 9X，Linux 等，配置好网关、代理等即可使用网络。图 1 给出了实验室网络拓扑。

代理服务器把实验室内部 Intranet 和外部 Internet 隔离开来，屏蔽内部网络的 IP 地址和应用服务器，具有多层安全机制，动态过滤出入代理服务器的数据包，若有异常可跟踪访问和随时报警。Microsoft Proxy Server 具有完善层次结构型缓存机制（Hierarchical Caching），支持分布式缓存队列（Distributed Cache Arrays），能够智能地、主动或被动地缓存大量访问过的网页内容，使后继用户访问命中率高，从而大大减少网络对 Internet 的访问流量。使用其构建具有防火墙和 WEB 高速缓冲功能的代理，可有效地提升访问 Internet 的性能和降低连接费用。

图 1　Internet 开放实验室拓扑

数据库服务器将代理日志存放于数据库，记录用户访问 Internet 的数据流量，作为计费和分析系统的原始数据。Microsoft Proxy Server 提供了完整的数据跟踪功能，不论向 Intranet 流入还是向 Internet 流出的数据流量，代理服务器均可以作出详细的记录资料。日志可以记录在一个文本文件，但考虑到计费管理和查询的方便，一般同时记录到一个提供 ODBC 接口的数据库（如 Microsoft SQL Server，Access，FoxPro 等）表中。动态包过滤时，协议冲突、数据包丢失等意外情况也记录到 Windows NT 系统日志中，可以查看以作出进一步优化。由于 SQL Server 与 NT 安全特性集成于 Back Office 家族，有利于安全管理和数据分析，建议采用。

IC 卡服务器连接带小键盘的 IC 卡读写器，控制对用户卡中剩余金额进行操作。在计算网络资源使用费用的时候访问数据库服务器，取得用户访问 Internet 的进出数据流量，按照不同价目计费。用户上下机时两次打卡，首次验证身份并记录开始时间，末次自动计算费用并从用户卡中扣除。

WEB 服务器主要用于向用户发布一些公共消息，以及提供用户费用查询的界面。使用和 NT 紧密集成的 IIS（Internet Information Server），编写 ASP（Active Server

Pages)数据库查询页面,通过 ADO(ActiveX Databasc Objects)和 ODBC 接口访问 SQL Server,查询结果动态生成页面返回客户。

其他各类信息服务器如邮件、FTP 等,由于和使用 IC 卡管理 Internet 开放实验室系统关系不大,在此不做介绍。但是作为方便用户使用的配套信息设施,这些服务器都应对 Intranet 内部开放。图 2 给出了各服务器的作用和相互关系。

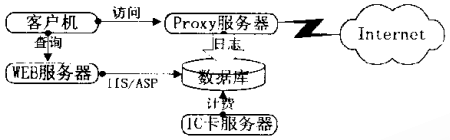

图 2 各服务器信息关系

以上各服务器实现上可以共用一台或几台主机,根据实验室的经费、配置等情况因地制宜。但代理服务器负担比较重,最好能够使用单独一台高级 PC 机担任。而 IC 卡服务器要求速度快,能迅速计算出用户本次上机消费金额并从卡中扣除。

三、计费管理策略

1. 用户管理

Proxy 帐户的用户管理建立在 Windows NT 的域安全模型之上,同 NT 的域用户管理、IIS 的安全机制紧密集成。Proxy Server 可以安装在独立服务器上,也可以在主域控制器上,提供了用户管理方面的极大灵活性。代理的帐号与 IC 卡 ID 一致或保持简单对应关系,以便快速计算用户费用。开户或者向现有 IC 卡加钱工作虽然可以由操作人员完成,但由于接触现金,最好有专人负责。数据库服务器中设立一个出纳数据库处理往来帐目,并有严格的存取权限设置以确保杜绝安全漏洞存在。

2. 收费

用户上机费用由使用机时、上网统计和上次节余三部分构成。在下机时 IC 卡服务器自动计算出本次该用户应缴纳的费用,从 IC 卡中扣除。根据用户要求,还可打印开销详细清单,确保收费合理性。同时,本次上机收入帐目变动情况以工作经营日志的形式存储到出纳数据库中,供有关人员据此进行帐目核对。本部分程序需要开发人员编制,是系统正常运作的核心模块。

(1)使用机时。当用户将 IC 卡插入读写器时,相关的用户识别信息被读出送往计费服务器主机。主机记录卡号,并询问个人密码。用户在读写器小键盘上输入密码,进行身份验证,如果通过,则上机开始时间同时被记录。在下机上,比较时间差再乘以机时单价(可设置),可得本次上机使用机时费。

(2)上网统计。上网费用由网上信息流量和各种信息费率共同决定。信息流量由 IC 卡服务器从访问日志数据库取得,并将取过的信息记录行打上已计费的标记,防止重复收取费用。Microsoft Proxy Server 提供的代理访问日志有访问时间、用户 ID、目的地、发送流量、接收流量、协议等 22 个信息字段,可准确详细地记录各用户活动情况。各种信息费率由管理员维护,可分为校内、国内各大网、国际以及白天、黑夜等多种款项,有些项目目前并不收取费用,但为兼容以后的发展和变化,可作保留而将费率设为 0。

(3)上次节余。在查询数据库以取得信息流量数据时,由于 Proxy 服务器并非实时地将代理日志记录在数据库中,可能有部分访问记录尚未存储入数据库。根据数据库收取的费用,可能有少许遗漏。故在计算本次信息使用费时,需要同时查询上次网络使用情况,将未作已计费标记的记录合并计算为上次节余款项,以做到公平合理地分摊 Internet 信息费用。

3. 查询

查询统计是 IC 卡计费系统的重要功能。系统应该提供给用户以完善简捷、易于使用的查询界面,及时反馈用户的访问信息情况和计费情况。用户可以根据查询结果核对上机情况,并及时调整上机工作。此外,管理人员也可以动态掌握各客户使用情况和服务器当前工作状态。

功能实现上,可以在 WEB 服务器主页中提供通用查询界面,让用户按照口令进入。按照不同帐号权限,可查询用户档案表、使用明细表、计费价目表等任意组合情况,比如:某段时间访问地址、应缴费用、代理总流量、目前用户等多项综合统计信息。

参考文献

[1] 王爱英著,IC 卡技术入门,清华大学版,1998

[2] Microsoft, SQL Server 程序员手册,宇航出版社,1997

[3] J. C. Crain, J. Webb 著, Visual Basic 5.0 Development's Workshop,机械工业版,1998

(来稿时间:1999 年 4 月)