

基于 Linux 系统的分布式网络管理系统

魏 晓,胡金初

(上海师范大学 数理信息学院,上海 200234)

摘 要:实现了一个基于 Linux + MySQL + Apache + PHP 开发的分布式网络管理系统,能够同时对多个不同服务器和网络设备进行管理和控制,实现统一用户管理、实时计费、收费以及查询等功能,极大地简化了网络的管理。

关键词:网络管理系统;用户管理;网络计费;分布式系统

中图分类号:TP393.07

文献标识码:A

文章编号:1673-629X(2007)06-0060-04

A Distributed Network Management System Based on Linux System

WEI Xiao, HU Jin-chu

(Mathematics & Science College, Shanghai Normal University, Shanghai 200234, China)

Abstract: A distributed network management system based on Linux + MySQL + Apache + PHP is realized. It can manage and control different servers or network devices at the same time, realize unified user management, real time accounting, charging, querying and etc, which predigest network management very much.

Key words: network management system; user management; network accounting; distributed system

0 引言

随着计算机网络在我国的迅速普及,各大、中、小学校和企业都已经或即将建成 Intranet 并接入 Internet,但是大家都面临着一个共同的问题,即没有一种界面友好、适合本单位网络实际情况的网络管理系统,网络管理复杂而低效^[1,2]。笔者根据我校实际情况开发了一套分布式网络管理系统,可以在一定程度上解决这个问题。

我校校园网通过 Cernet 接入 Internet,向校园网用户提供 WWW, FTP, Email, Proxy, PPP, BBS 和直接 IP 地址访问 Internet 等服务。校园网用户可以在不同的服务器上申请不同的服务,可以通过 Proxy 访问 Internet 或者拥有可直接访问 Internet 的 IP 地址。这样用户信息就分布于不同服务器中,而且针对不同用户、不同的服务需要采取不同的收费标准,从而造成了计费策略复杂,用户使用比较麻烦,例如用户要分别设置不同服务的密码等等。为了实现对用户集中控制、简化用户管理及对各服务器和网络设备的统一管理,设计并开发了该系统。

收稿日期:2006-08-22

基金项目:上海市教委科研基金(050203)

作者简介:魏 晓(1973-),男,安徽宿州人,讲师,硕士研究生,研究方向为网络与多媒体技术;胡金初,教授,硕士生导师,研究方向为计算机网络。

1 系统设计

1.1 系统要求

校园网上的服务器都是基于 Linux 操作系统的,为了便于操作和管理,要求在 Linux 上实现基于 WEB 界面的网络管理系统,系统应实现以下功能:

(1) 统一的用户界面。

用户可能申请了多个不同的服务,要求将分布于各服务器的用户信息集中,以便能够统一地管理用户信息,实现网络用户统一身份认证等功能,以简化用户的操作。同时要向用户提供帐户状态控制(用户能够自主暂停和启用某种服务、修改密码、设置每月的消费限额等)、信息查询(用户能够查询当前的帐号状态、服务状态、实时帐单、访问历史、交费历史等)等服务。

(2) 统一的管理界面。

因为服务器和网络设备的分布位置分散和软件系统的差别,管理员需要单独管理每个服务器和网络设备,这是相当复杂和麻烦的。为简化管理和屏蔽不同设备的差别,要求在统一的 WEB 界面下实现用户控制、收费及对多种不同的服务器和网络设备的控制,这样普通的管理员即可实现对系统的控制,既方便了管理又可以缓解技术人员不足的问题。

(3) 实时、自动计费。

要求能够根据不同的用户类别和不同的服务项目采取不同的计费策略,实时对多种不同的服务自动计

费。

(4) 自动控制。

要求根据用户状态变化自动停止(如欠费、暂停等)和开启(交费等)用户在各服务器上的服务。

1.2 设计思想

上述功能有多种不同的实现方法^[3,4],例如目录服务等可以实现用户的统一认证,但不是所有的服务都支持 LDAP 协议,为此按照如下方法来实现这些功能。

选择一台服务器安装 Linux + MySQL + Apache + PHP 作为管理服务器。采用 MySQL 数据库作为系统的中心数据库,所有用户的数据及系统运行数据都存于该数据库中。通过 WEB 方式提供用户界面和管理员界面,通过 WEB 界面操纵中心数据库进而控制各服务器。

各受控服务器上运行专门的代理进程负责定时读取中心数据库信息,根据其中用户状态和控制信息对服务进程进行控制,同时把本服务的日志上传至管理服务器,并写入中心数据库中。

管理服务器的后台进程定时处理来自各受控服务器的数据,根据计费策略进行计费,按照计费结果进行用户状态和控制信息的设置。

对网络设备管理时,因为有的设备无法安装自己开发的代理程序,为此设置一个专门代理服务器,由该服务器根据各网络设备的具体情况采用 SNMP 协议等网络管理协议实现与设备间的通信,将设备状态传至系统中心数据库,将管理员通过综合管理界面的命令发送给各受控网络设备。

通过这种方式,用户和管理员只要通过 WEB 界面管理即可,而由位于各服务器的代理进程实现各服务器与管理服务器的通信及对各服务器进行控制,这样就简化了用户的使用和管理员的对用户的管理;由网络设备管理代理服务负责管理员和网络设备之间的交互,简化了管理员对网络设备的管理。

1.3 系统模型

按照上述思想实现了如图 1 所示的系统模型,是由管理服务器、分布于各受控服务器上的代理控制程序以及网络设备管理代理服务器等构成的分布式管理系统。

1.4 数据库设计

运行于 Linux 上的 MySQL 数据库具有许多优点,如安全性可以防止非法用户访问、大容量可以容纳数十亿条记录、高速可以保证较好的系统响应^[5,6]。正是

因为这些优点选择了 MySQL 数据库作为系统的中心数据库。

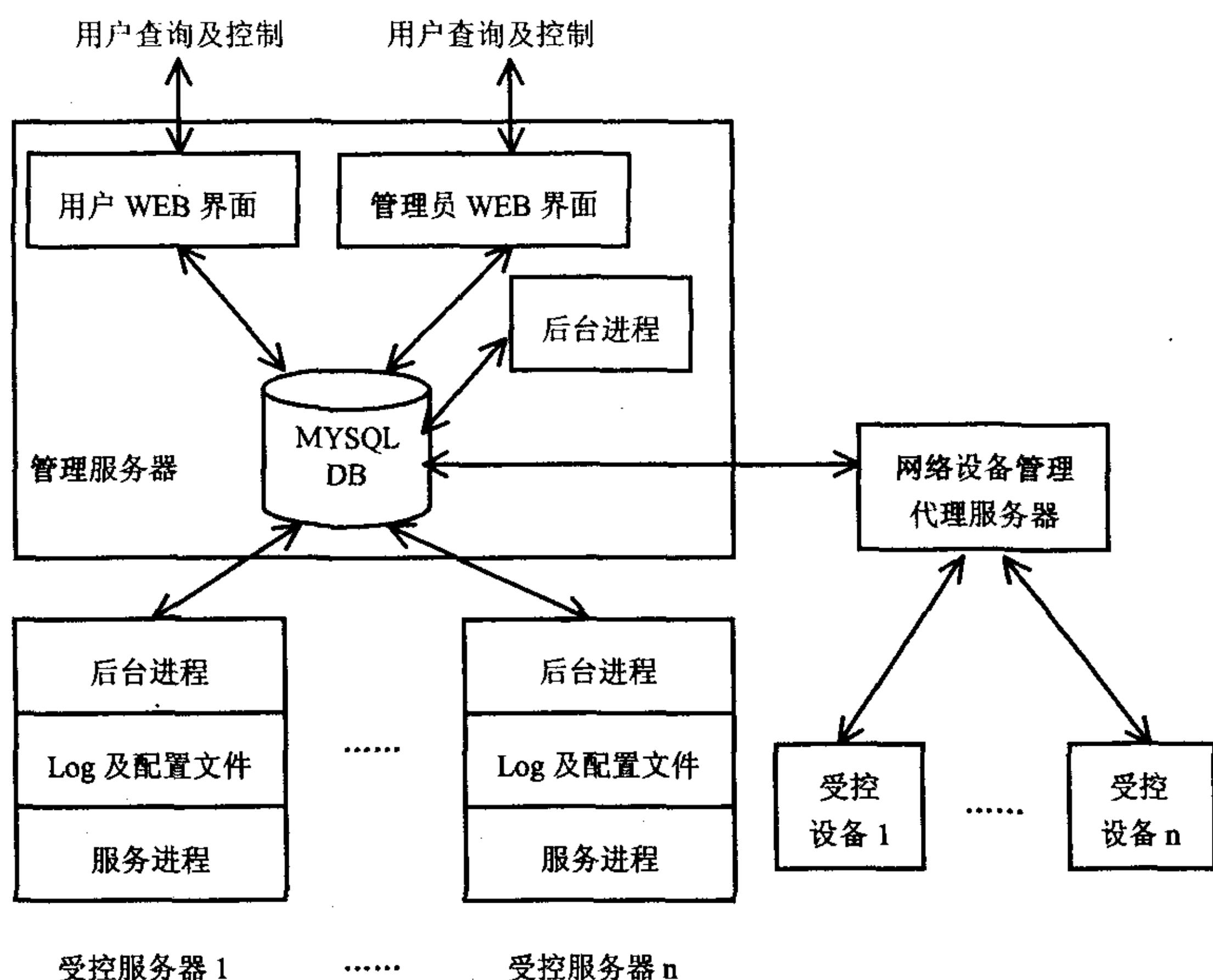


图 1 系统模型

根据需要,网络管理系统的数据库由以下数据表构成:

- (1) User: 用户信息表,保存注册用户基本信息、密码、申请服务、注册 IP、用户状态及用户控制信息等。
- (2) Admin: 管理员表,存储管理员的各种信息,对管理员进行身份认证。
- (3) Role: 管理员角色表,定义了管理员的角色,是系统权限管理的基础。
- (4) Baserate: 计费策略表,保存不同身份用户的各种服务的费用标准及各种优惠策略等。
- (5) Monthrate: 月计费表,按月存放用户的各种费用,其中本月的费用为动态增加的实时费用。
- (6) Accesslog: 访问日志表,详细记录用户使用各种服务的信息,如代理访问记录、电子邮件记录、PPP 拨号记录、IP 访问记录等,供用户和有关部门查询。
- (7) Oplog: 操作记录表,记录管理员和用户数据库的详细操纵记录,如修改密码、交费、状态控制等,是系统安全的一个部分。
- (8) Control: 控制规则表,存放对各服务的控制规则信息。
- (9) DeviceCommand: 设备控制指令表,存放对各网络设备进行控制的指令。
- (10) Freeip: 免费地址列表,记录免费 IP 地址,是系统计费的依据。

1.5 WEB 界面设计

为了方便用户和管理员的操作,用户和管理员界面采用 WEB 界面实现,这样就可以实现在网络上允许

任一台计算机上实现对系统的管理。考虑到系统以 MySQL 数据库为核心,所以选择了 Apache 作为 WEB 服务器、PHP 语言作为脚本语言。因为 PHP 的最大优点就是对数据库的操作方便,PHP 和 MySQL 的完美结合使开发相当方便。

(1) 网络用户界面。

管理系统通过 WEB 界面给网络用户提供密码修改、查询和状态控制等方面的功能。用户通过密码修改界面修改的密码仅是中心数据库中的用户密码,用户在各服务器中的密码要等到系统同步以后才能生效,一般为 5 分钟左右。用户通过查询功能可以查看注册信息、访问记录、实费费用、交费历史信息、用户状态等信息。

状态控制功能提供给用户控制用户状态的功能,用户可以在暂停、注销、启用等几个状态之间转换,用户可以方便有效地管理个人帐户,一些操作可以在网上由用户自助完成,既方便了用户也简化了管理员的工作。

(2) 管理员界面。

通过 WEB 界面给不同级别的管理员提供用户维护、收费、用户状态控制、费率设置、服务器控制、网络设备管理、数据备份、数据统计等功能。

①用户管理功能包括新增用户、注销用户、修改用户信息、修改用户帐号状态等功能。既可以单个用户管理,也可以批量管理。可以由外部 EXCEL 表中导入批量数据对用户进行管理,这在新生入学需要建立大批用户时非常方便。也可以通过指定查询条件对查询得到的一批用户进行某种操作来实现对用户的批量管理。灵活的用户管理方法,能够满足校园网用户数多、大批量变动等特点。

②系统策略管理功能。网络管理系统的许多配置参数都在系统策略管理功能中实现。包括:计费策略,即设定多种不同身份的网络用户,并给不同用户的不同服务指定不同的收费标准;系统同步的周期,即指定各分布系统与中心数据库同步的周期;收费地址列表,指定需要收费的地址列表,作为计费的依据。

③服务器及网络设备管理。提供统一的管理界面对各服务器和网络设备进行管理,包括查看服务器状态、起停服务和设备等。

④收费管理。提供网络使用费的管理界面,包括交费、退费、费用统计等功能。

⑤数据备份。对系统数据库进行备份,可以设置自动备份的周期,也可以通过界面手动备份。

这些功能中的需要涉及其它服务器和网络设备的先是由 PHP 脚本对管理服务器的中心数据库的相应

数据进行操纵,真正生效要等到各受控服务器中的控制程序和网络设备代理完成同步以后,所以有一定的延迟。

(3) 用户及角色管理。

用户登录基于 WEB 界面的管理系统时,系统对管理员用户采用了基于角色的分级用户管理机制,系统的默认角色有:

- * 超级管理员,该组用户具有系统的各种权限。

- * 网络设备管理员,能够进入设备控制界面,查看设备状态,对各设备发送指令。

- * 网络用户管理员,能够管理网络用户,新增,注销,管理网络用户状态。

- * 收费管理员,能够进入收费界面进行收费及收费统计。

- * 系统策略管理员,能够进入系统策略管理界面,进行策略管理。

- * 数据备份管理员,能够完成数据备份任务。

管理员用户可以隶属于以上一个组或多个组,也可以随时改变当前身份,从而具有不同的操作权限,这样就可以方便地对管理员进行管理。各管理员登录系统时,系统根据管理员的当前角色进行操作权限的分配,管理员进行角色转换后,重新分配用户的操作权限。

1.6 管理服务器后台程序

管理服务器的后台程序需要定时处理来自各受控服务器的数据,考虑到系统的响应时间要求,选择 C 语言来实现,该后台进程定时从数据库中取出各受控服务存入的数据,处理数据,根据不同的服务类型、用户类型进行计费,并把统计结果存入各用户记录中,判断用户状态并设置用户状态字段。

此后台程序是系统中很重要的一部分,它一直按计划后台运行,负责系统的绝大部分数据处理功能。因为校园网的用户数量大,每一分钟各服务器产生的日志量相当大,后台程序必须在下一次启动之前完成对大量日志的分析、计费及对用户状态的设置。

该后台进程的启动周期的设置与系统的反应速度和数据量都有关系。周期大则表现为系统的反应慢,用户或管理员在 WEB 界面设置的一些操作,必须经过后台处理程序运行以后才能同步到各受控服务器中,周期越大数据同步的受控服务器上的时间越长,也即响应速度越慢。反之周期小则导致后台程序频繁启动,对系统的性能造成影响。

除了设置恰当的启动周期以外,还应该仔细设计计费算法,以减少系统处理大量数据的速度,提高系统的响应速度。

1.7 网络设备管理代理服务

因为某些网络设备无法运行单独开发的代理进程,而各网络设备又采用不同的协议和方法通信,如果在管理系统直接增加模块和各网络设备交互,则会导致网络管理系统独立性降低,当增加网络设备时,网络管理系统也需要做相应的修改。

在系统中单独设置一个网络设备管理代理服务,该服务可以运行在一个独立的计算机上,也可以安装在网络管理系统的同一宿主计算机上。该代理服务按照各网络设备的要求安装多协议,实现和网络设备的交互,获得网络设备状态和日志,向网络设备发送指令。代理服务把获得的日志和设备状态格式化以后写入网络管理系统的中心数据库中,同时读出其中设备管理员发出的对网络设备管理的指令并发送到相应的网络设备。由此网络设备管理代理服务成为网络管理系统和网络设备之间的桥梁。

当网络设备发生了变化,只要修改代理服务的相应部分即可,因为代理服务只负责网络设备和管理系统之间的通信,不具有其它功能,所以修改代理服务程序要比修改整个网络管理系统更容易实现。

1.8 受控服务器代理程序

各受控服务器代理控制进程定时运行,取本服务的日志,通过网络写入管理服务器数据库中,同时读取管理服务器 User 表中的用户状态信息和 Control 表中本服务的控制信息,对本服务进行控制,对用户进行控制。根据不同的服务类别有不同的控制方式:

(1)代理服务器:对欠费、暂停和消户的帐号进行删除;对新注册、重新交费等用户的追加帐号;根据控制信息对外屏蔽某些 Internet 站点,对内封某些 IP 地址禁止使用代理;起停代理服务等。

(2)电子邮件服务器:对欠费、暂停和消户的帐号进行暂停收发信件;对新注册用户追加帐号。

(3)路由器:根据用户状态,屏蔽和开放某些内部 IP,根据控制信息屏蔽和开放某些外部 IP。

(4)WWW 和 FTP 服务器:不计费,只是根据用户状态,增加帐号,暂停某些帐号。

1.9 系统安全

该系统从以下方面对系统进行保护,在一定程度保护了系统的安全:

(1)数据库安全。通过密码保护和 IP 地址限制,

防止非法客户端连接 MySQL 服务器。通过注册用户分级,对不同的数据表有不同的权限,防止注册用户的越界使用。

(2)用户数据安全。通过用户登录和详细操作记录保护用户数据。

(3)管理权限保护,管理员分级,根据不同的权限进入不同的 WEB 页面及详细的操作记录,对管理权限进行保护。

(4)数据传递安全。在各服务器间传递的重要控制信息先加密后传送。

(5)数据备份。对系统数据库进行自动和手工备份,备份可以在本地进行也可以在远程进行。

2 结 论

该系统以 MySQL 数据库为中心实现了对多种异构服务器的控制和用户管理,对网络设备的统一管理,具有较好的可扩充性,当增加新服务时,只要针对该服务开发代理程序即可纳入整个系统中使用。当然系统也存在不足,如系统存在延迟,当用户修改密码,或设置控制信息后必须等到受控服务器进程下一次启动后方能生效。对此可以设置受控服务器代理进程的运行频率来改善,另外对于管理员下达的控制信息可以通过立即启动代理进程来响应,这样在一定程度上提高系统的响应能力。

该系统全部基于免费软件开发实现,成本低,可维护性好,已经在我校网络中心正式使用,运行效果好。

参考文献:

- [1] 郑发杰,胡谷雨.一种可扩展的分布式网络管理系统的实现[J].军事通信技术,2004,25(3):1-4.
- [2] 陆慧娟,曹 贞.基于 Linux 的企业 Webmail 系统[J].微机发展,2004,14(5):19-21.
- [3] 李 莉,王 平.一种基于事件检测的分布式网络管理系统模型[J].东北大学学报,2002,23(7):613-616.
- [4] 王 薇,吴宇红.分布式网络管理系统中的访问控制[J].计算机仿真,2005,22(1):135-137.
- [5] 兰旭辉,熊家军,邓 刚.基于 mysql 的应用程序设计[J].计算机工程与设计,2004,25(3):442-443.
- [6] 张 飞.利用 MySQL 构建分布式应用[J].计算机工程与应用,2001,37(18):102-104.