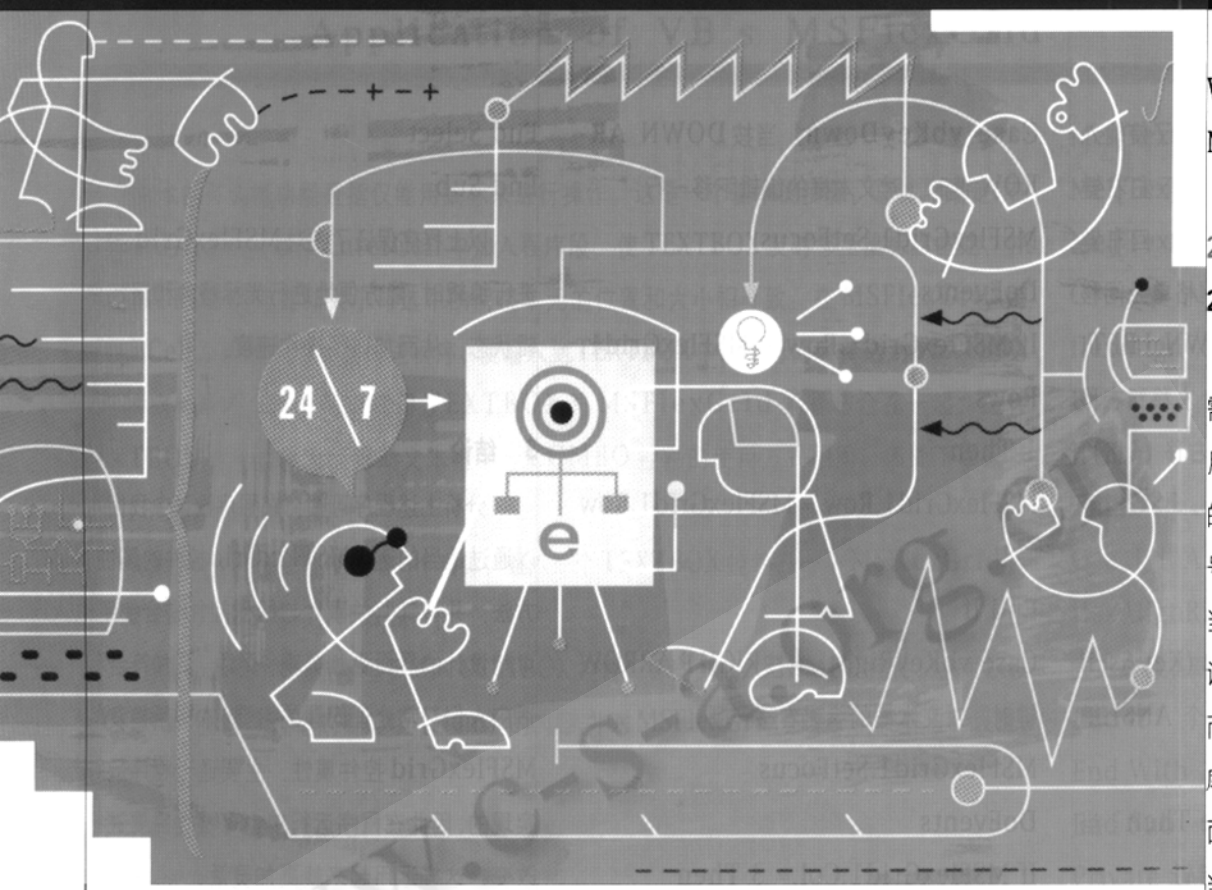

代理服务器在校园网中的应用

Application of Proxy Server in Campus Network

钟嘉鸣 （湖南郴州师专网络中心 423000）

摘要：在分析代理服务器概念和工作原理的基础上，就校园网环境，以MS Proxy Server2.0为例，阐述了代理服务器的防火墙安全性、Cache缓存、Web发布等功能的实现方法，并对如何利用代理服务器的日志功能开发校园网计费管理软件问题进行了探讨。

关键词：代理服务器 Internet IP

1 引言

随着校园网接入CERNET/Internet，网络用户日益增多，网络规模不断扩大，对网络安全可靠、高效运行提出了更高要求。如何监控网络，以了解、掌握网络运行状况，控制网络信息，对不良信息进行过滤，保证校园网应用的健康发展，如何有效保护网络资源，特别是校园网内部资源，如何加快网络访问速度，降低一些不必要的费用，这些都是网络管理中要解决的问题，也是校园网管理的难题。根据我们的实践，代理服务器的使用可有效地解决这一难题。

代理服务器软件种类很多，有Netscape Proxy Server，Microsoft Proxy Server，Wingate等，我校采用了Microsoft Proxy ServerV2.0。

2 代理服务器概述

2.1 概念

代理服务器就是当网络用户需要访问Internet资源时，代理用户向所要访问的站点索取资料的一个服务器。需要送出请求信号，取得回应，然后再传送回来。当设定了代理服务器后，用户的请求信号会先送到代理服务器，而代理服务器就好像一个大储藏库，它有一个很大的磁盘缓存，里面储存着用户以前访问过的资料，当代理服务器得到用户的请求时，首先会到缓存中寻找有没有同样的资料，如果有，用户发出的请求信号就不会送到远端的目的服务器，而是由代理服务器直接将资料传给用户。

2.2 代理服务器的工作原理

代理服务器实际上是一台安装了代理软件的机器，它负责捕捉某个端口的数据包，然后把请求转发到相应目标的IP和端口，取得需要的数据后，再送回发出请求的地址。代理软件由服务器端程序与客户端程序组成，它一般不允许内部网（Intranet校园网）与外部网（Internet）之间直接通信。若内部用户需访问外部网，首先内部用户和代理服务器之间建立通信连接，然后代理服务器再与外部网的服务器建立通信连接。硬件实现是这样的：在代

理服务器中安装两块网卡，其中一块通过路由器与Internet相连，其地址是真实的IP地址，由它实现校园网与Internet的连接；另一块网卡则通过交换机与校园网内部各客户机相连，并由它给每个客户机分配一个虚拟的IP地址，实现客户机与Internet的间接相连，从而共享Internet资源。可见，代理服务器是内部网和外部网之间的一个关联设备，如图1所示。

3 代理服务器的功能

3.1 防火墙功能

代理服务器作为防火墙，一方面是由于它将所有跨越防火墙的网络通信链路分为两段，防火墙内外计算机系统应用层的"链接"由两个终止代理服务器上的"链接"来实现，外部计算机的网络链路只能到达代理服务器，从而达到了隔离防火墙内外计算机系统的作用。另一方面它还可以通过包过滤、域过滤、用户授权和安全警报与日志等措施保证使用代理服务器的校园网安全性。

3.1.1 包过滤

包过滤功能在网络层为校园网提供安全保护，它可以严格控制通过代理服务器进入和外出的IP数据包。同别的包过滤防火墙不同，PROXY SERVER提供的动态包过滤（Dynamic packet filtering）可同时支持流入和流出包过滤，动态决定哪一个数据包可进入校园网络和应用层代理服务，动态包过滤能够在接、发数据时自动打开通信端口，在代理服务器终止连接后立即关闭通信端口，从而能够减少代理服务器上暴露端口的数量和每个端口打开的时间，从而可以提高网络的安全性。设置包过滤的基本步骤为：

(1) 选择"开始"→"程序"→"Microsoft Proxy Server"→"Microsoft Management Console"，弹出MMC界面。

(2) 在MMC中，单击"Web Proxy"，右击，在弹出菜单中选择"属性"项，在弹出的"Web Proxy Service Properties"对话框中选择"Service"选项卡，然后单击"Security"按钮，弹出"Security"安全设置对话框，选择"Packet Filters"，弹出包过滤设置对话框。

(3) 选择"Enable packet filtering on external"复选框，使对外部数据的包过滤生效。

(4) 如果使用动态包过滤，选中"Enable dynamic packet filtering of Microsoft Proxy Server packets"复选框；如果要过滤自带寻址信息的数据包或数据包片，则选中"Enable filtering of IP fragments"复选框。

(5) 可单击"Add"、"Edit"和"Remove"来增加新的过滤器或编辑和删除列表框中的包过滤器，设置完后单击"确定"退出。

3.1.2 域过滤器(Domain Filters)

代理服务器的使用为校园网用户提供了很大方便，但INTERNET上的站点浩如烟海，有大量反动、淫秽的信息。另外，由于CERNET的特殊收费方式：既有免费IP站点，又有收费IP站点，所以如何控制或是禁止对某些INTERNET站点的访问是一个十分重要的问题。

PROXY SERVER在这方面提供了域过滤器（DOMAIN FITERS）功能，可以通过IP地址、子网掩码、域名方式来控制访问INTERNET站点。域过滤的作用是限制校园网用户对INTERNET的访问，管理员可以指定用户访问的INTERNET站点。当代理服务器接收到用户以域名方式提交的请求时，它把域名解析为IP地址，然后把用户访问站点的域名和IP地址同过滤中指定的站点进行比较，从而决定是否允许访问。如果以IP地址的方式向代理服务器发出访问请求，代理服务器首先在过滤中查找是否有访问的IP地址，如果代理服务器中有以域名方式建立的过滤条件，访问的IP地址将被反向解析为域名，并与域过滤器进行比较，以判断是否允许访问INTERNET。设置域过滤器的基本步骤如下：

(1) 选择"开始"→"程序"→"Microsoft Proxy Server"→"Microsoft Management Console"，弹出MMC界面。

(2) 在MMC中，单击"Web Proxy"，右击，在弹出菜单中选择"属性"项，在弹出的"Web Proxy Service Properties"对话框中选择"Service"选项卡，然后单击"

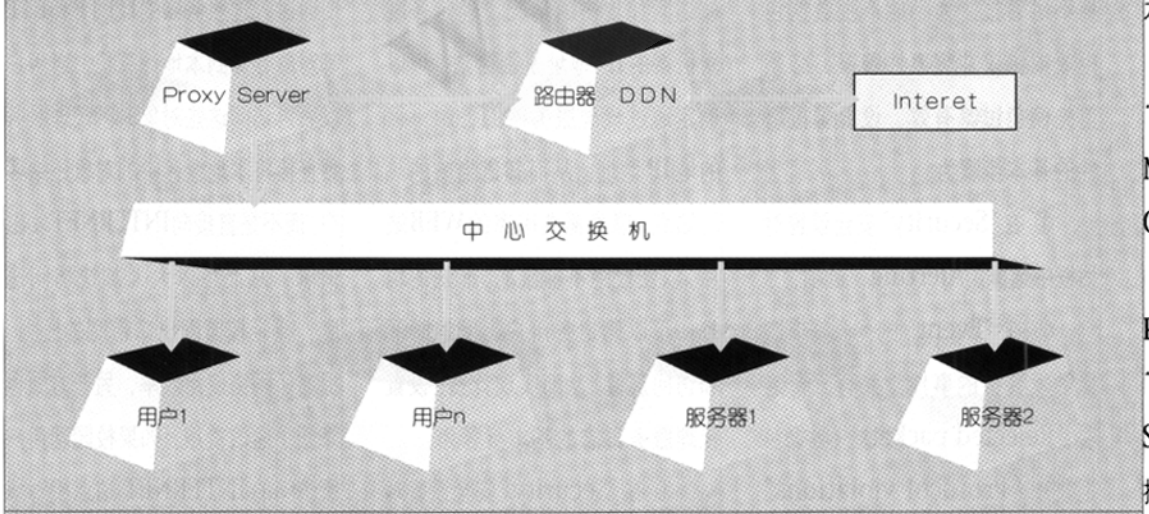

图1

Security"按钮，弹出"Security"安全设置对话框，选择"Domain Filters"，弹出域过滤器选项卡。

(3) 选择"Enable Filtering"项，然后选择过滤模式，有两种基本方式可供选择，如果要禁止访问某些站点，则首先选择"Granted"，然后在"Except to those listed below"中添加要禁止访问的站点，则除了在"Except to those listed below"中填入的站点外，校园网用户可以访问所有其他的Internet站点；如果要允许访问某些Internet站点，则首先选择"Denied",然后在"Except to those listed below"中填入允许访问的站点，则除了该表中所列的站点外其他站点校园网用户将被拒绝被访问。

(4) 如果要建立新的允许或禁止访问的Internet站点，则选择"Add"，出现三种选择：采用域名过滤"Domain"、单一IP地址过滤"Single Computer"及一组IP地址过滤"Group of Computer"三种方式，其中：(I)域过滤"Domain"，管理员可以输入需要过滤的域名。如要将用户访问的站点限制在国内，则输入"*.cn"实现；(II)单一IP地址过滤"Single Computer"，必须输入要限制访问计算机的IP地址；(III)一组IP地址过滤"Group of Computer"，则必须输入该组计算机的IP地址和子网掩码。设置完成后，单击"OK"保存以上设置。

(5) 单击"Edit"和"Remove"可编辑或删除IP地址和域名列表。单击"确定"退出。

3.1.3 安全警报和日志

(1) 使用Proxy Server可以监控可疑的网络事件，如拒收的数据包，协议冲突或日志存储空间不足。这些事件被记录在包过滤日志和Proxy Server服务日志中，也可选择放在Windows NT的系统事件日志中或者以E-mail方式发给特定的接收者。Proxy Server提供了安全事件的实时通知功能。

抛弃的数据包和变形帧将触发数据包拒收事件，如果在某一时间范围内，一个数据包被抛弃的频率很高，表示网络很可能受到了非法攻击。可以设定数据包拒收的频率，达到该频率后，Proxy Server将产生一个警报事件。当过滤的数据包或帧不符合允许的协议格式时，将触发协议冲突警报事件，表示网络也可能受到外来攻击。当磁盘所存储的服务日志或数据包日志超过规定的磁盘容量时，将触发磁盘容量不足警报。为了能产生数据包拒收或协议冲突事件警报，必须首先使包过滤有效。设置警报事件的基本步骤为：

① 在"Security"安全设置对话框中选择"Alerting"选项。

② 在"Event"的列表框中选择触发警报的事件，共有三个选项："Rejected packets"(数据包拒收)、"Protocol violations"(协议冲突)和"Disk full"(磁盘空间不足)。

③ 选择"Generate system event if more than "，然后输入每秒钟产生的事件频率数，如果超过了该频率数将产生系统事件。

④ 如果想把警报作为一个E-mail信息发出，则选择"Send SMTP Mail"复选框；如果想把警报送到Windows NT系统事件日志，选择"Report to Windows NT Event Log"复选框。在"Delay before next report"中输入一个以分钟为单位的数值，表示与下一个报告产生之间的延迟。

⑤ 单击"Configure mail"可设置接收事件警报的E-mail参数，单击"Reset Defaults"恢复默认的警报参数设置。

⑥ 单击"确定"按钮退出。

(2) 因为校园网中的INTERNET通信都通过代理服务器，代理能够记住所有的请求，并将其存入日志中。分析日志文件可以使网络管理员了解校园网被访问和攻击的情况；确定各联网机器的IP地址是否合法；可以确定通过代理服务器的各源、目的地IP地址，从而知道当前的热门站点，隔离需要隔离的WEB站点，以便杜绝不健康的、非法的信息；可以确定各用户上网的时间和访问流量，从而实现计费。设置代理服务日志的基本步骤为：

① 在"Security"安全设置对话框中选择"Logging"选项。

② 选中"Enable logging using"复选框，然后从右边的列表中选择日志格式，共有两种："Regular"(常规)和"Verbose"(详细)。

③ 设置日志的存放方式："Log to file"(存放到文件)或"Log to SQL/ODBC database"(存放到SQL/ODBC兼容数据库)。

④ 选择"Log to file"后，接着设置日志是否自动使用同一日志文件、老日志文件的限定数和日志文件存放路径和文件名等参数。

⑤ 如果选择"Log to SQL/ODBC database"，接着输入该数据库的ODBC数据源名DSN、数据表、用户名和口令。

⑥ 全部设置完后，单击"确定"退出。

3.2 cache缓存功能

我校校园网通过64KDDN专线与CERNET省网络中心相连，随着用户的增加，这将成为INTERNET通信的一个瓶颈。由于PROXY SERVER提供的缓存功能使通过代理服务器的HTTP和FTP等对象存储到本地计算机，当用户以后再访问这些对象时，代理服务器直接将本地缓存中的对象还给客户，而不是直接向INTERNET发出请求，从而可以大大加快访问速度，减轻校园网出口带宽的压力，提高了网络使用效率，另一方面也降低了通信费用。如果校园网用户所访问的INTERNET站点相对集

中，校园网用户越多，代理服务器带来的效果就越明显。设置缓存的基本步骤为：

(1) 在"Web Proxy Service Properties"对话框中选择"Caching"选项。

(2) 选择"Enable caching"复选框，使缓存有效。

(3) 在"Cache expiration policy"下设置被动(passive caching)的过时(expiration,即缓存对象是否有效)策略。设置被动缓存的有效期共有三种选择："Updates are more important"(维护缓存数据的最新性，这样可能增加服务器访问Internet的负担)，"Equal importance"(在缓存数据的最新性和缓存性能之间寻求均衡)和"Fewer network accesses are more important"(用户使用缓存的频率很高，要求较快的反映速度)。

(4) 选择"Enable active caching"复选框，可设置动态缓存。

(5) 单击"cache size"设置缓存数据区的大小。

(6) 单击"确定"退出。

3.3 WEB发布功能

利用代理服务器提供的反向代理功能和IIS结合，在不妨害校园网安全的情况下，可以在校园网内部向INTERNET发布信息，即PROXY SERVER可以反向代理外部用户对内部网络的访问，如果校园网内部的某些主机允许外部用户访问时，可以把这些主机站点建立在防火墙里面，这样既能方便校园网内部用户的访问，又能对外发布信息，扩大学校在社会上的知名度。

在"Web Proxy Service Properties"对话框中选择"Publishing"选项，选择"Enable Web Publishing"，使Web发布有效，为了使外部用户访问校园网，首先必须建立外部访问地址映射表，当注册过的外部用户提交请求时，代理服务器将把外部用户的访问请求直接转到指定主机。对未建立映射的外部访问请求，有三种选择：

① discarded(抛弃外部访问映射表无法映射的访问)；

② sent to local web server(将外部访问映射表无法映射的访问转到代理服务器的本地web服务)；

③ sent to another web server(将外部访问映射表无法映射的访问转发到一个指定的web服务器进行处理)，然后输入服务器名和端口号。

单击"Default Mapping"可设置默认Web服务器主机；单击"Add"可增加反向主机路由，建立外部URL和校园网内部主机的映射。单击"确定"按钮退出。

4 基于代理服务器的计费软件的实现

我们可以利用代理服务器的日志文件开发计费管理软件，具体做法如下：

(1) 在后台搭建MS SQL Server7.0数据库服务器，在SQL Server中建立一个数据库Account，其中建立一个表Account-LOG-TABLE，记录WWW、WinSock等代理活动。

(2) 在代理服务器上使用管理工具MMC设置好Web Proxy、Winsock、Socks Proxy等服务，在"Logging"选项卡中，设置日志的存放方式为"Log to SQL/ODBC database"，配置好该数据库的ODBC数据源名DSN、数据表、用户名和口令。这样可以通过ODBC将访问日志信息导入到上述数据表中。

(3) 前台使用Delphi5.0开发计费管理软件，Delphi应用程序通过BDE与SQL Server7.0建立连接。该程序的主要功能为：用户管理、费用查询、打印、统计分析、费率设置等。其中费用采取按流量计费的政策，费用=费率*流量(流量以kb为单位)。具体流程图如图2所示。

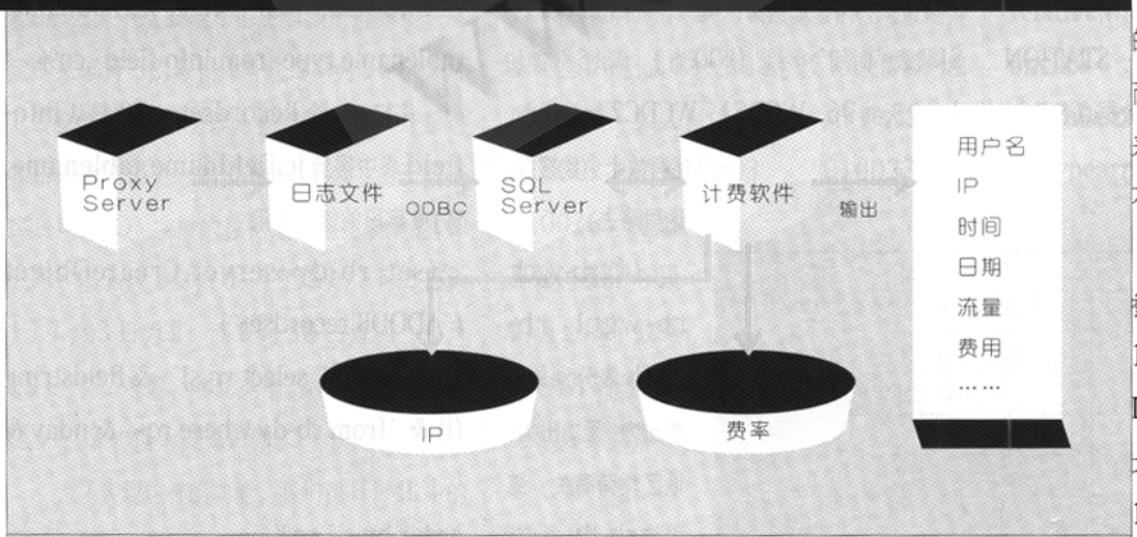

图2

5 结束语

代理服务器是网络管理中非常重要的工具，它不仅在校园网的管理中发挥着日益明显的作用，而且在整个网络领域也得到了越来越广泛的应用，同时其功能也不断完善和发展。

参考文献

1 李明柱等，Windows NT中Intranet组建和管理技术[M]，北京北京航空航天大学出版社，1999。