网络监听在基于网络流量计费中的应用

陈国震
(浙江纺织服装职业技术学院　宁波 315111)

摘　要　利用网络监听对机房运行进行有效流量计费的管理，从而提高管理效率和服务质量。本软件系统中采用层次化、模块化、对象化的方式构建软件平台，采用了C/S结构，使得系统具有良好的可扩展性。

关键词　机房流量计费，管理效率，服务质量，网络监听

Application of Network Sniffer in Network Account Based on Network Flow

CHEN Guo-Zheng
(Zhejiang Textile & Fashion College, Ningbo 315111)

Abstract　The software can manage the valid discharge charge for the computer room with network sniffer in order to increase management afficiency and service quantity. It adopts the method of hiberarchy, modularization and objectization to set up a softwares platform, adopting the C/S construvtion to make system with good expanding.

Keywords　Computer room discharge charge, Management efficiency, Service quantity, Network Sniffer

1　引言

随着计算机的发展，人们对计算机教育的需求越来越迫切，高校的计算机数量也越来越多，机房开放可以避免资源浪费。但机房缺少网络流量计费管理，不能为学生提供基于网络流量的详细信息计费，手工的方式进行计费，容易出错而且工作繁重，计算机的使用对学生并没用任何限制，容易造成逃费。采用基于网络流量的计费管理可以避开以上缺点，减轻管理员工作量，提高管理效率和服务质量[1]。

2　系统方案设计

本文所研究的机房网络流量计费管理系统主要解决以下问题：

1)获取流量：实现网络流量计费，必须先解决每台机器在任一时间段内的网络数据流量。得到上网计算机使用的网络流量最好的办法是通过获取该机器的发送/接收的IP包来进行。系统获取IP包是通过采用高效的流量捕捉程序来采集各个网段的网络流量，并按照各个计算机、流量的类型(HTTP服务、Mail服务、FTP服务、Telnet服务等)进行分类，按照设定的时间周期性地入库。然后对需要计费的网络流量，按照网络管理员设定的计费标准实现对流量的计费。

2)帐户管理：基于流量的网络计费软件还要求对流量按上网用户进行分类汇总记入用户的帐户上。通过防火墙过滤规则设定帐户，对合法的用户给与放行，从而实现帐户管理。不需要管理员干预，系统会自动管理已经登记的合法用户。客户端用户输入帐号和口令，计费系统就可开始统计流量，当用户下机后，计费系统将该用户的网络流量记入该用户的帐户上，同时记录用户的网络服务类型和时间等信息，并释放资源。管理员或用户在WEB业务查询端，查询网络流量、计费情况等，因为这些处理所涉及的数据都在数据库中，可以通过WEB服务器来实现。见系统结构图1所示。

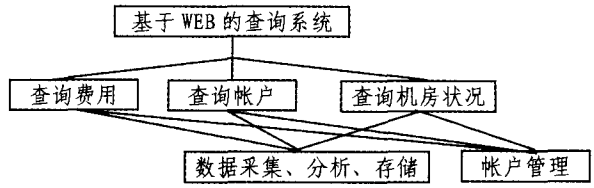

图1　系统结构

3　网络流量采集/计费的分析设计

实现网络计费通常有三种方式：(1)使用代理服务器方式；(2)使用路由器内部功能来实现计费；(3)网络监听计费。如图2(网络计费图)所示。

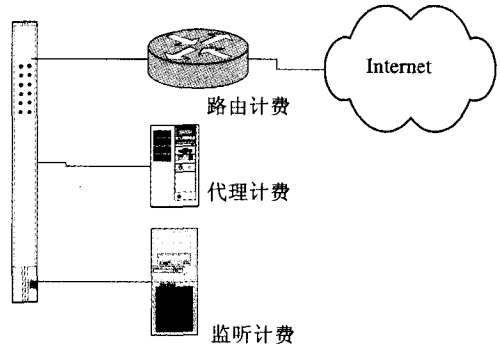

图2　网络计费图

(1)代理服务器计费：通过代理服务器的日志功能来进行计费。这种情况，可以在代理服务器上安装一个计费程序，从日志中读取数据进行计费。

(2)路由器计费：通过路由器本固有的功能来实现计费。路由器是内网和外网连接的通道，内网与外网之间的网络流

陈国震　实验师，主要研究方向为计算机网络安全。

量都必须经过路由器。所以是计费软件采集流量数据的地方,大部分路由器都具有流量记录的功能。计费系统把这些流量信息从路由器中读出来,经过程序处理生成按每个 IP 地址流量的计费帐单。

(3)网络监听计费:通过监听网络上的数据,进行分析,存储。这种计费方式与路由器计费方式相同,只是把数据采集,分析,存储工作交给监听服务器来完成。以下着重讨论网络监听计费。

3.1 流量采集系统的分析和设计

计费信息的采集包含两大部分:数据的捕获及分析处理。

(1)数据的捕获。

利用 WinPcap[4] 捕获数据包:WinPcap 是一个开源的、运行于 Win32 平台的体系结构,它的主要功能是进行捕获和网络分析。WinPcap 包括了内核级别的包过滤、低层次的动态连接库(packet. dll)、高级别系统无关的(wpcap. dll)等。本系统利用 WinPcap 中提供的函数对流经网卡的数据包进行捕获。具体步骤如下:

1)获取设备列表

获取网络接口设备列表可以调用 WinPcap 提供的 pcap_findalldevs_ex()函数。

2)打开网络接口

打开网络接口设备可以使用 WinPcap 提供的 pcap_open()函数。

3)在打开的网络接口卡上捕获网络数据包

WinPcap 提供了多种不同的方法捕获数据包,其中,pcap_dispatch()和 pcap_loop()通过回调函数将捕获的数据包传递给应用程序,而 pcap_next_ex()则不使用回调函数。

由于最底层的工作由 WinPcap 驱动完成,只需要将它捕获的数据包收集起来,而且这个工作要不间断,并保证不丢弃数据包。通常需要创建一个工作者线程(CapturerThread)负责网络数据包的接收工作。在接收到网络数据包后,工作者线程通过发送消息等机制通知另一线程处理接收到的网络的数据包。用线程(CapturerThread)来实现收集功能,并赋给它高的优先级,为提高效率,数据捕获时不是逐个数据包的收集,而是以若干个数据包组成的缓冲区为收集单位。

定义的数据结构:

```
typedef struct FrameHeader_t {
BYTE DesMAC[6]; //帧首部
BYTE SrcMAC[6]; //目的地址
WORD FrameType; //源地址
}FrameHeader_t;
typedef struct IPAddr {
unsigned char AddrByte[4];
};
typedef struct IPHeader_t {
BYTE Ver_HLen;
BYTE TOS;
WORD TotallLen;
WORD ID;
WORD Flg_Segment;
BYTE TTL;
BYTE Protocol;
WORD CheckSum;
struct IPAddr SrcIP;
struct IPAddr DstIP;
};
typedef struct Data_t{
FrameHeader_t FrameHeader;
IPHeader_t IPHeader;
}Data_t;
```

接收数据包线程 CapturerThread 从网卡设备上读取数据报文,及将其放入缓冲区。

```
CapturerThread * CapturerThread = new CapturerThread(true);
CapturerThread->Resume(); //请求同步
```

(2)分析处理。

首先考虑对监听的数据按端口和服务进行分类。第二,存储和管理收集到的数据包。第三,分析数据包的流量信息需要定时保存。第四,完成分析功能。

3.2 流量采集过程分析

采集系统的工作流程。

第一,采集程序初始化:启动客户端和服务器连接的通信模块,服务器的认证和防火墙过滤规则,进入采集初始化。通过安装的动态连接库(PACKET. DLL)直接访问 BPF(分帧过滤器)驱动程序,打开管理员所设定的采集网络设备,并设置其工作模块为混杂模式,以便于它截获数据包。同时指定包的大小和设置相关结构[5]。

保存截获的数据包结构定义如下:

```
typedef struct DataPack
  {int port; //端口号
      unsigned_int32 FlowS; //总流量
      unsigned_int32 SendS; //发送流量
      unsigned_int32 ReceivS; //接收流量
  }Portinfo;
```

第二,启动数据包的分析线程:它通过调用安装的动态连接库的导出函数 PacketReceivePacket 来接收 Winpcap 驱动捕获的数据包缓冲,把它拷贝到定义数据的缓冲区中,从缓冲区中取下一个包,调用分析服务。若无包可分析就休眠。分析过程如下:接收的数据包是带 Bpf 头部的以太网帧。先取出 Bpf 头部信息,找出以太网帧的头部,判断是否是 IP 包,如果是 IP 包,则提出 IP 的头部信息,查出此包的协议类型(TCP/UDP/ICMP 等)、源 IP 地址和目的 IP 地址以及源端口号和目的端口号,按照头部信息中的数据长度作为该数据包的最终长度,按端口号和类型分类流量数据写入帐户数据库中。部分程序如下:

分析数据包类型的代码段如下:

```
if (FormM->swaps(EtherHead->FrameType)==ETHER_PRO-
  TOCOL_IP) //分析出以太网 IP 数据报文
{……
if(IPHeader_t->Protocol==6) //TCP(6)
{
…… //协议值为 6,即是 TCP 的数据报文
}
if(IPHeader_t->Protocol==17) //UDP(17)
{
…… //协议值为 17,即是 UDP 的数据报文
}
if(IPHeader_t->Protocol==3) //ICMP 的数据报文
{
…… //协议值为 3,即是 ICMP 的数据报文
}
……
```

判断目的端口值,FTP(文件传输协议)21、TELNET(远程登录)23、SMTP(简单邮件传输协议)25、http (WWW)80、POP3(邮局协议)110 等。

分析数据包端口的代码:

```
switch(FormM->swaps(TCPHead->DstPort)) {
case 21: p=FormM->port[0]; break; //ftp(command send)
case 80: p=FormM->port[2]; break; //http
case 6666: p=FormM->port[4]; break; //icq
case 200: p=FormM->port[9]; break; //ftp(send data)
case 23: p=FormM->port[1]; break; //telnet
case 8000: p=FormM->port[3]; break; //oicq
case 139: p=FormM->port[5]; break; //Neighbor
case 110: p=FormM->port[6]; break; //pop3 (receive mail)
case 25: p=FormMain->port[7]; break; //smtp send mail)
case 1433: p=FormMain->port[12]; break; //sql server
default : p=FormMain->port[11]; break; //all 的 IP pack)
}
```

数据库表如下:

表1:时间　源地址　源端口　目标地址　目标端口　协议　包数量　流量

表2:源地址　源端口　目标地址　目标端口　协议　包数量　净流量　发出流量　接收流量　捕获时间

系统WEB查询界面:如图3所示。

班级 04模具　用户名 林华

时间	源地址	源端口	目标地址	目标端口	协议	包数量	流量
16:21	220.181.28.42	4001	172.16.1.10	4000	UDP	1	210
16:21	220.181.28.42	4001	172.16.1.10	1660	UDP	1	290
16:21	220.181.28.42	4001	172.16.1.10	1665	UDP	2	350
16:21	61.153.17.56	21	172.16.1.10	1650	UDP	1	300

图3　计费查询

4　帐户管理

服务器端采用ASP语言编写,读取客户端提交的用户名和口令,通过查询数据库来验证用户名与口令是否正确,并与防火墙进行通信,完成授予用户访问Internet的权限。用户授权功能通过调用防火墙来实现,即动态的修改防火墙的过滤规则,通过认证的用户的数据包通过。图4用户认证和授权图。

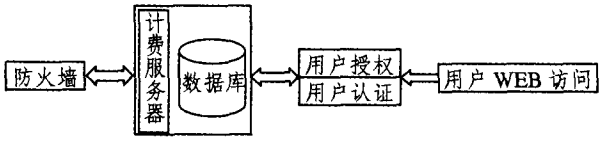

图4　用户认证和授权

总结　本文主要研究了如何利用网络监听实现流量管理,将计费原始信息功能集成到一个完整系统,从而对机房运行进行有效的管理,提高管理效率和服务质量。并给出了部分代码和设计思想。基于网络流量计费的机房管理有着比较重要的现实意义。能实现:

1. 机房老师在自己的办公室通过浏览器访问收费管理页面,实时的监督学生上机情况,查询学生信息和收费人员管理情况。

2. 学生上机非常方便,直接进入机房寻找空余计算机,录入自己的帐号及口令即可。不会发生机房拥堵和混乱。

3. 由于帐号及费用的管理在浏览器上进行,完全抛开了空间距离的影响。机房老师在进行日常教务工作同时即可进行计费系统的管理。

4. 机房老师的体会:上机的人多了,收益明显提高了,自己反而更轻松了。

5. 不用人工干预,计算机能自动地实现网络流量的计费。

参考文献

1　朱晟,等. 实验室教学改革与培养学生创新能力的实践与思考[J]. 实验室研究与探索,2001(4):17～18

2　张军. 基于Windowns环境下的NPF数据捕获技术的研究. 计算机科学,2005(5)

3　井口信和. TCP/IP网络工具篇. 科学出版社,2003(4):63

4　张建忠,等. 计算机网络实验指导书. 清华大学出版社,2005,1:8

5　宋军. 显式流量控制协议XCP研究. 计算机科学,2005(7)

(上接第49页)

参考文献

1　Madden S, Franklin F J, Hellerstein J M, et al. TAG: A Tiny AGgregation Service for Ad-Hoc Sensor Networks. OSDI, 2002

2　Madden S, Franklin M J, Hellerstein J M, et al. The design of an acquisitional query processor for sensor networks. ACM SIGMOD, 2003 (To Appear)

3　Faradjian A, Gehrke J, Bonnet P. GADT: A Probability Space ADT For Representing and Querying the Physical World. ICDE, 2002

4　Trigoni N, Yao Y, Demers A, et al. Wavescheduling: Energy-efficient data dissemination for sensor networks. In Submission, June 2003

5　Intanagonwiwat C, Govindan R, Estrin D. Directed diffusion: A scalable and robust communication paradigm for sensor networks. Mobi-COM, Boston, MA, August 2000

6　Madden S, Franklin M J. Fjording the stream: An architechture for queries over streaming sensor data. ICDE, 2002

7　Bonnet P, Gehrke J, Seshadri P. Towards sensor database systems. Conference on Mobile Data Management, January 2001

8　Yao Y, Gehrke J. The cougar approach to in-network query processing in sensor networks. SIGMOD Record, September 2002

9　Yao Yong Gehrke J. Query processing in sensor networks. Proceedings of the First Biennial Conference on Innovative Data Systems Research (CIDR), 2003

10　Madden S, Szewczyk R, Franklin M, et al. Supporting aggregate queries over ad-hoc wireless sensor networks. WMCSA, 2002

11　Madden S, Shah M A, Hellerstein J M, et al. Continously adaptive continuous queries over data streams. ACM SIGMOD, Madison, WI, June 2002

12　http://telegraph.cs.berkeley.edu/tinydb, TinyDB's main page

13　Tamer M, Valduriez O P. Principle of Distributed Database Systems Second Edition

14　Madden S, Franklin M J, Hellerstein J M, et al. TinyDB: an acquisitional query processing system for sensor networks. ACM Trans. Database Syst. 2005,30(1): 122～173

15　Trigoni N, Yao Yong, Demers M J, et al. Hybrid Push-Pull Query Processing for Sensor Networks. GI Jahrestagung 2004(2): 370～374

16　Bonnet P, Gehrke J, Seshadri P. Querying the Physical World. Cornell University

17　Ratnasamy S, Karp B, Li Yin, et al. GHT: A geographic hash table for data-centric storage. In: Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks (WSNA), 2002

18　Li X, Kim Y J, Govindan R, et al. Multi-dimensional range queries in sensor networks. In: Proceeding of the First ACM Conference on Sensor Systems(SenSys), 2003

19　Hill J, Szewczyk R, Woo A, et al. System Architecture Directions for Networked Sensors. In: ASPLOS, 2000. 93～104

20　JIN Che-Qing, QIAN Wei-Ning, ZHOU Ao-Ying. Analysis and Management of Streaming Data: A Survey. Journal of Software

21　Akyildiz I F, Su W. A Survey on Sensor Networks

22　Levis P, Madden S, Gay D, et al. The Emergence of Networking Abstractions and Techniques in TinyOS. NSDI, 2004. 1～14

23　Gehrke J, Madden S. Query Processing in Sensor Networks Sensor and Actuator Networks

24　Hellerstein J M, Wei Hong, Madden S, et al. Beyond Average: Toward Sophisticated Sensing with Queries. In: IPSN, 2003. 63～79

25　Trigoni N, Yao Yong, Demers A J, et al. Multi-query Optimization for Sensor Networks. In: DCOSS 2005. 307～321

26　Demers A J, Gehrke J, Rajaraman R, et al. The Cougar Project: a work-in-progress report. SIGMOD Record 2003,32(4): 53～59

27　Heidemann J S, Silva F, Intanagonwiwat C, et al. Building Efficient Wireless Sensor Networks with Low-Level Naming. In: SOSP 2001. 146～159

28　Motwani R, Widom J, Arasu A, et al. Query Processing, Approximation, and Resource Management in a Data Stream Management System. CIDR 2003

29　Chandrasekaran S, Cooper O, Deshpande A, et al. Continuous Dataflow Processing for an Uncertain World. CIDR 2003

30　Abadi C D, et al. Aurora: a new model and architecture for data stream management[J]. The VLDB Journal, 2003, 12

31　Al-Karaki J M, Kamal A E. Routing techniques in wireless sensor networks: a survey

32　Madden S. The Design and Evaluation of a Query Processing Architecture for Sensor Networks: [Ph. D Thesis]. UC Berkeley, Fall 2003

33　Krishnamachari B, Estrin D, Wicker S B. The Impact of Data Aggregation in Wireless Sensor Networks. In: ICDCS Workshops, 2002. 575～578

34　Deshpande A, Hellerstein J M. Lifting the Burden of History from Adaptive Query Processing. In: VLDB, 2004. 948～959

35　Garofalakis M, Gibbons P. Approximate query processing: Taming the terabytes! (tutorial). In: VLDB, 2001

36　Chakrabarti K, Garofalakis M, Rastogi R, et al. Approximate query processing using wavelets. VLDB Journal, 2001(10)