# 高效率多线程网络流量采集算法研究及实践

袁梅宇
(昆明理工大学 信息工程与自动化学院, 云南 昆明 650051)

摘要: 介绍了采用 SNMP协议采集 CISCO路由器网络流量的方法, 对流量采集算法进行了分析, 提出一种高效率的流量采集算法. 创建四个线程进行数据采集和处理: 发送线程、接收线程、预处理线程和存储线程. 发送线程负责发送 SNMP请求报文, 接收线程负责接收 SNMP响应报文, 预处理线程过滤及整合采集到的流量信息, 存储线程负责将预处理后的数据持久地存入数据库中. 由于采用并行方式进行数据采集, 该算法较串行采集效率高, 并在实践中验证其可行性.

关键词: 网络流量; SNMP协议; CISCO路由器
中图分类号: TP393. 07 文献标识码: A 文章编号: 1007- 855X(2006)01- 0032- 05

# On the High Efficiency Multithreading Net Flow Collection Algorithm and Relevant Practice

YUAN Mei-yu
(Faculty of Information Engineering and Automation, Kunming University of Science and Technology, Kunming 650051, China)

**Abstract**: Methods of using SNMP Protocol to collect net flow by addressing CISCO router are introduced. Net flow collection algorithms are carefully analyzed. An efficient net flow collection algorithm is proposed. Four threads are created to handle data collection and data processing whose functions are sending, receiving, pre-processing and storing up the thread. Sending thread takes responsibility of sending SNMP request messages, while receiving thread takes charge of receiving SNMP response messages. Due to the fact of parallel data collection, the algorithm is sure of high efficiency. Pre-processing thread filtrates and processes raw data, and stores thread feeds data into databases. The approach has already been verified in practice.

**Key words**: net flow; SNMP protocol; CISCO router

## 0 引言

作为网络管理系统的五大功能之一, 计费管理能够监测和控制网络操作的费用、代价, 记录网络资源的使用情况. 因此, 入网单位、ISP准确地掌握网络资源的使用情况是做好网络管理工作中的重要前提.

网络流量采集是计费管理的基础. 网络流量的变化可综合反映诸多网络运行中故障、性能等方面的信息. 只有准确、及时地采集并记录网络流量信息, 才有可能进行正确的计费; 只有通过对网络运行的历史流量信息记录的科学分析, 才有可能为网络管理人员提供高层决策(网络可靠性分析、网络升级、网络拓扑变化)的支持, 才有可能对上网节点信息(节点上网时间、网卡地址、IP地址、端口)、服务器服务状态、网络通断等信息进行管理. 所以, 研究网络流量信息采集算法具有现实意义.

网络流量采集的方法有多种[1], 但最为简便的是启用路由器自身的功能来记录流量信息, 再通过网络管理协议(如 SNMP)来实现流量信息的采集、汇总. 路由器是园区网连接 Internet的通道, 是信息出入的咽喉. 企业网到 Internet的全部网络流量都必须经过路由器, 反之亦然. 所以采集流量数据最佳的方式就是启用路由器的相应功能(现在一般的路由器中都有记录流量的功能). 网络流量信息通过路由器时, 其

收稿日期: 2004- 10- 10.
作者简介: 袁梅宇(1967. 9~), 博士. 主要研究方向: 网络技术, 分布式计算. **E- mail**: mkyuan_98@ sohu. com

流量信息都会在路由器的内存中保存下来.流量信息一般包括四个字段:源 IP地址、目标 IP地址、包数和字节数.计费策略中,通常按照字节数来进行计费,这是最为合理的计费方式[2].

SNMP(Simple Network Management Protocol,简单网络管理协议)[3~5]是 IAB(Internet Architecture Board, Internet体系结构委员会)在 1988年正式制定了为 TCP/IP协议集所采用的网络管理协议标准.SNMP协议最大的优越性在于其通用性.虽然 SNMP的初衷仅是作为临时标准,但它日益发展,已经得到广泛应用,获得广泛的支持,成为事实上的标准,基于 SNMP保证了计费系统的通用性和可重用性.大部分路由器都支持 SNMP协议,因此,本文采用 SNMP协议采集路由器流量信息的方案.

## 1 CISCO流量采集的方法

CISCO路由器是国内目前使用最广泛的网络设备,它支持 SNMP,并且能记录流量信息.利用 SNMP的 GetRequest和 GetNextRequest遍历整个计费 MIB(Management Information base,管理对象信息库)表就可以得到通过该路由器的流量信息.这种方法的优点是计费软件可移植性高,可以对不同厂家路由器进行计费,而不需要改动或少量改动计费软件.

CISCO路由器维护两个与 IP计费有关的数据库,一个是活动数据库(active database),一个是检查点数据库(checkpoint database).活动数据库实时地记录所有经路由器转发的 IP流量数据,每当接收到一个 checkpoint命令时,路由器首先清空检查点数据库,接着把活动数据库的数据拷贝到检查点数据库中,然后清空活动数据库.上述过程相当于对当时的网络流量保存了一份快照.这两个与计费相关的表存在于 CISCO MIB的 IP组中,它们分别是 local IP accounting table——lipAccountingTable和 local IP Checking Accounting table——lipCKAccountingTable.

IP accounting table(1.3.6.1.4.9.2.4.7.1)提供读取活动数据库数据的变量,它包含下面几个变量:actSrc(1):源 IP地址;actDst(2):目的 IP地址;actPkts(3):从源到目的包流量;actByts(4):从源到目的字节流量;actViolation(5):从源到目的的包违背的访问列表号,0表示没有违背任何访问列表;actAge(9):当前数据的生命期(以为 Timeticks单位). IP accounting table的索引变量是 actSrc和 actDst其中 actSrc, actDst, actPkts, actByts都是和计费相关的变量.

CISCO MIB的 IP Checking Accounting table(对象标识 OID为 1.3.6.1.4.9.2.4.9.1)提供读取检查点数据库数据的变量,包含以下几个列变量:ckacSrc(1):源 IP地址;ckactDst(2):目的 IP地址;ckactPkts(3):从源到目的包流量;ckactByts(4):从源到目的字节流量;ckactviolation(5):从源到目的的包违背的访问列表号,0表示没有违背任何访问列表;ckactAge(11):当前数据的生命期(以 Timeticks为单位). IP Checking Accounting table的索引变量是 ckacSrc和 ckactDst其中 ckactSrc, ckactDst, ckactPkts, ckactByts是和计费相关的变量[6].

另外,在 IP组中还有一个与计费有关的变量:actCheckpoint(对象标识 OID为 1.3.6.1.4.1.9.2.4.11.0).读入该变量(SNMP GetRequest)然后把它重新设置(SNMP SetRequest)为同一值,就可以激活检查点数据库.系统这时就会把活动数据库中的数据转移到检查点数据库中,并把活动数据库清空.这时 IP Checking Accounting table中就包含有最新的流量信息的快照,可以通过 SNMP GetRequest(或 GetNextRequest)循环读取计费信息.

## 2 流量采集算法分析

通过前面的分析,我们知道对路由器流量信息的采集需要如下步骤:

1)发出 SNMP GeRequest命令读入 actCheckpoint变量的值,并将该值作为 SNMP SeRequest命令的参数置入 actCheckpoint使之翻转;

2)使用 SNMP GetNextRequest命令循环读入 IP Checking Accounting table中的计费信息;

3)改变 IP地址指向下一个路由器,循环至 1,直到所有路由器采集完毕.

从上面步骤可以推断:单线程的流量信息采集可以分为两个循环,外循环遍历网络中需要采集的路由器,内循环遍历路由器计费信息记录.单线程采集多个路由器是串行方式,由于受路由器响应时间和网络迟延的影响,采集效率必然会很低.

提高采集效率的改进思路是采用并行方式,同时启动多个线程进行采集.

如图 1所示,忽略网络冲突和数据帧丢失,从效率上比较,串行单次采集所需要的平均时间 $\Delta s$由下式决定:

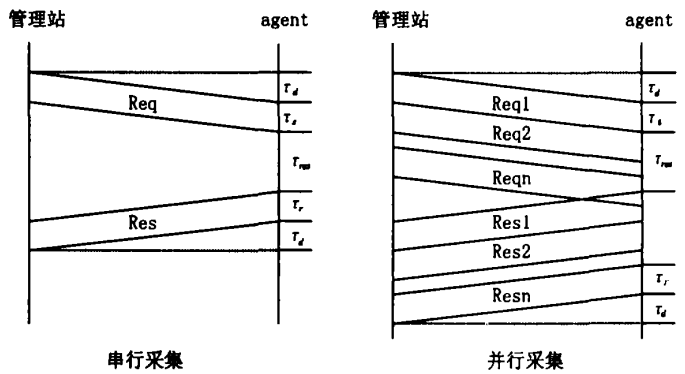
$$\Delta s = \tau_d + \tau_s + \tau_{res} + \tau_r + \tau_d \quad (1)$$

相对而言,并行采集平均采集一个路由器所需要的时间 $\Delta p$ 由下式决定:

$$\Delta p = (N * (\tau_d + \tau_s) + \tau_{res} + \tau_r + \tau_d) / N \quad (2)$$

其中,$N$ 为需要采集的路由器数目.

根据文献[5],在局域网中,Agent(这里指路由器)的处理时间约为 50ms级别,网络延时(1 000字节的数据包,无明显阻塞)大约 1ms,因此可以忽略 $\tau_d$、$\tau_s$、$\tau_r$.则(1),(2)式分别变为:




其中,$\tau_d$:传播迟延,$\tau_s$:发送 SNMP 请求报文平均时间,$\tau_{res}$:平均响应时间,$\tau_r$:发送 SNMP 响应报文平均时间

**图1 串行采集和并行采集比较**

**Fig.1 Comparison of serial data collection and parallel data collection**

$$\Delta s = \tau_{res} \quad (3)$$

$$\Delta p = \tau_{res} / N \quad (4)$$

由(3)、(4)式可知并行采集所花费的时间明显要少.

在极端的情况下(如路由器发生故障),管理站一般需要重发 SNMP命令多次(通常为三次)无响应后才能确定路由器故障.并行采集所花费的时间显然比串行采集所花费的时间少,因为前者等待多个路由器响应的时间是并行的(即重叠的)而不是串行的.

多线程并行采集可以采用下列方案:

第一、采用与路由器数目相同的采集线程来进行并行采集.但这种方案有一些缺点:如果需要采集的路由器数目过多,启用相同数目的线程消耗的资源也相应较大,会对系统的运行效率产生不良影响,而且频繁创建(new)新线程或杀死(kill)线程也会使系统开销过大.再则,动态网络变更也挑战其算法的灵活性和适应性.

第二、提高效率的改进方案是采用线程池.该方案与数据库连接池的原理类似,基本原理是:在采集程序启动时固定地启动数个(参数可调)线程,并行地循环采集多个路由器.在一轮采集完成后(或者所有未完成采集的路由器都已经分配到采集线程),已启动的空闲线程并不终止,而是休眠(sleep),等到下一轮采集时,再唤醒采集线程.

## 3 高效率的流量采集算法

本文提出一种高效率的多线程流量采集算法,称之为“收发双线程采集”,该算法已经在实际项目中得到应用.

采集程序运行在一台管理站(计算机或工作站)中.采集进程中创建的线程有:一个发送线程、一个接收线程、一个预处理线程和一个存储线程,这些线程都由一个主控线程控制.发送线程负责发送 SNMP请求报文,接收线程负责接收 SNMP响应报文,预处理线程过滤及整合采集到的流量信息,存储线程负责将预处理后的数据持久地存入数据库中.

收发双线程采集主要工作原理是,待发送的 SNMP请求报文在任务队列中排队,任务队列可采用先进先出或其它优先级的排队方式. 当发送线程发送完一个 SNMP请求报文后,就从任务队列取出新的 SNMP请求报文并发送,直到任务队列为空. 接收线程负责监听 SNMP响应报文,它一直处于活动状态. 一旦接收到响应报文,接收线程进行简单的身份鉴别(即认证,检查 Community字段)后就将其放入一个缓冲区,我们称该缓冲区为"RawNetFlowBuffer",然后唤醒预处理线程对其进行处理. 预处理线程处理完后,将处理过的数据(称为"一次数据")放入另一个缓冲区,这个缓冲区称为"FirstDealtNetFlowBuffer". 最后存储线程定时周期性地将一次数据存入数据库中,供将来查询和生成账单使用.

本采集算法在实现上采用多线程技术,各线程各司其职,设计非常简明. 需要的注意的是:

第一、接收线程只负责接收数据,并存入缓冲区中,不进行多余的数据处理,时刻做好接收准备,等待新数据包的到来,以免造成数据包的丢失,引起超时重发而增加网络负载.

第二、由于发送线程不等 agent回应就发送多个请求数据包,这显然属于异步通信方式. 接受线程必须实现 SnmpClient接口,并在回调(callback)函数中实现接收响应数据包的逻辑.

第三、异步通信方式要求接收线程知道所接收的响应数据包是哪一个请求数据包的回应. 如果请求数据包和响应数据包都使用 ID进行标识,这个问题就可以迎刃而解. 幸运的是, AdventNetSNMP的 API工具包已经提供了这种功能. 因此,本文采用的方法是:在构造请求数据包 SnmpPDU时,通过 setReqid方法设置请求 ID(requestID). 这样,接收线程通过回调函数接收响应数据包时就可通过判断请求 ID,从而得知这是哪一个请求数据包的回应.

回调函数的原型如下:

```
public boolean callback(SnmpSession session, SnmpPDU pdu, int requestID)
```

其中,第三个参数(requestID)就是请求 ID.

第四、由于计费原始数据非常重要. 为保证不丢失数据,各线程的启动应按照一定的顺序,只有当预处理线程和存储线程都启动并且工作正常时,才能启动发送线程、接收线程来采集数据. 并且上述线程由一个主控线程通过定时发送采集信号进行控制.

为了方便理解,将收发双线程采集的主要流程用 UML活动图 2所示.

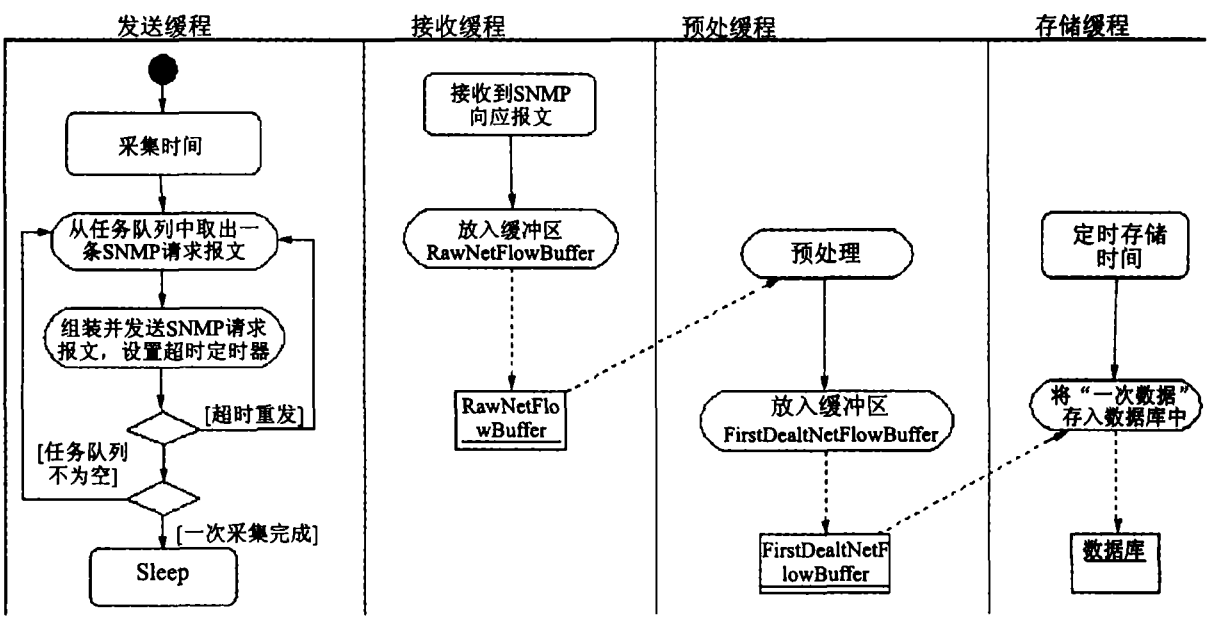



**图2　收发双线程采集的UML活动图**

**Fig.2　UML active diagram of dual threads collection**

收发双线程采集和采用线程池采集比较: 由于网卡是一个共享设备, 任一时刻只能有一个线程使用该网卡进行通信, 因此, 线程池采集不可避免地要进行多个采集线程之间的同步, 同步可以通过设立临界区或信号量加锁进行控制, 另外, 由于每个采集线程都可以采集路由器, 到底由谁来采集需要调度, 实现起来有一定的难度. 而采用收发双线程采集, 收、发线程独占网卡资源, 只需要开辟一些缓冲区作为线程间进行数据传输的临时空间, 算法较为简单, 调试也相对容易.

## 4 结束语

采用 SNMP协议和多线程采集路由器的网络流量信息, 符合标准, 符合网络管理的潮流, 运行效率高, 效果令人满意.

开发环境: JBuilder 8.0, AdventNetSNMP 3.3, Windows 2000.

参考文献:

[1] 李文印, 周治国, 张福春. 网络计费系统数据采集技术研究[M]. 计算机应用, 2003, 23(2): 2003.
[2] 赵小林, 高虹. 网络管理技术教程[M]. 北京: 国防工业出版社, 2002. 155~163.
[3] [美]马赛厄斯·海因, 戴维·格里菲斯. 简单网络管理协议的理论与实践 SNMP[M]. 邢国光等译. 北京: 国防工业出版社, 1999. 58~164.
[4] [美]Mani Subramanian. 网络管理——原理与实践(影印版)[M]. 北京: 高等教育出版社, 2003. 141~203.
[5] [美]William Stallings. SNMP网络管理[M]. 胡成松等译. 北京: 中国电力出版社, 2001. 168~192.
[6] Cisco System, Inc. MIB User Quick Reference [EDB/OL]. http://www.sisco.com.

(上接第 31页)

## 5 结 论

通过对生物质成型技术的技术经济评价及燃煤锅炉改造后的实际运行情况可以看出, 小型锅炉改造为生物质成型燃料锅炉在技术和经济上都是可行的, 它不仅解决了环境保护和农村生物质资源浪费的问题, 同时为我国在煤炭、石油等化石能源的替代产品方面寻找新的出路, 尤其是生物质能源在大型工业锅炉、窑炉等用能方面的需求. 所以, 燃用生物质成型燃料锅炉的产业化前景比较光明.

参考文献:

[1] 马孝琴. 生物质成型燃料燃烧动力学特性及液压秸杆成型机改进设计研究: [博士学位论文] [D]. 郑州: 河南农业大学, 2002. 20~25.
[2] 刘胜勇, 陈开碇, 张百良. 国内外生物质成型燃料及燃烧设备研究与发展现状[J]. 可再生能源, 1995, (4): 14~15.
[3] 吴添祖, 虞晓芬, 龚建立, 等. 技术经济学概论[M]. 北京: 高等教育出版社, 1998. 11~61.
[4] 万仁新. 生物质能工程[M]. 北京: 中国农业出版社, 1995.