第34卷 第20期 计 算 机 工 程 2008年10月
Vol.34 No.20 Computer Engineering October 2008
·网络与通信· 文章编号：1000—3428(2008)20—0124—03 文献标识码：A 中图分类号：TP393

分布式网络流量监测

刘军良，肖宗水
(山东大学计算机学院，济南 250061)

摘 要：分析2种现行网络流量监测技术：利用标准的网络管理方法记录IP流量和利用NETFLOW的方法进行流量统计。针对这2种方法的局限性，提出分布式网络流量监测方法。该方法采用Client/Server结构，局域网各个终端参加流量统计，并将结果传送给流量监测服务器。该方法适合大型局域网的流量监测，具有良好硬件适应性，大大降低了流量监测服务器的工作量，提高了网络性能。
关键词：网络流量；SNMP协议；分布式监测

Distributed Monitor on Network Traffic

LIU Jun-liang , XIAO Zong-shui
(School of Computer, Shandong University, Jinan 250061)

【Abstract】This paper analyzes two kinds of technology about network traffic monitor: scoring up traffic using the standard network monitor method and the NETFLOW method. For the defects of the two methods, it advances the distributed monitor on network traffic, uses the Client/Server structure. Every terminal in LAN joins monitor traffic and sends traffic data to the traffic monitor server. The fact demonstrates that this technology is suit for the traffic monitor of large LAN. It diminishes the work load of traffic monitor server distinguishably and elevates the performance of Internet, at the same time, it displays great adaptability for hardware.
【Key words】network traffic; SNMP protocol; distributed monitor

网络流量监测一直是网络技术研究领域的热点，其重要意义在于：网络流量监测是建立精确网络与业务行为模型、设计健壮网络协议、开发高性能网络设备的基础；实时网络流量监测可以及时发现网络流量异常、检测网络故障与攻击，从而提高网络运维水平、加强网络安全防范[1-2]；网络流量监测可以为流量工程实施、网络与业务规划设计提供科学依据。本文在研究网络流量监测技术现状的基础上，提出了一种基于客户端的分布式流量监测方法。

1 国内外研究现状

现行的主要网络流量监测技术有SNMP(Simple Network Management Protocol)方法和NETFLOW方法。

(1)利用标准的网络管理方法记录IP流量

目前，在整个网络管理领域，应用最广的协议标准是SNMP。计费管理作为ISO五大网络管理功能之一，采用标准的网络管理协议可以完成IP流量记录。

采用SNMP协议进行IP流量统计的方法要求流量记录和统计由计费服务器和路由器合作完成。遵照SNMP协议的工作原理，由计费服务器充当SNMP的manager，路由器充当SNMP的agent。其中，计费服务器定期向路由器发送SNMP请求snmpwalk，从路由器获取数据，本地处理数据，完成数据的存储、统计等功能，提供能直接为计费使用的数据格式，与计费服务器相配合的路由器除了完成一般路由器具有的路由转发功能之外，还要提供统计过往包的功能，并以MIB的形式存储在本地，以备manager随时查询。目前，Cisco公司在其路由器操作系统IDS中提供用于IP计费的MIB。原则上，其他厂商的路由器只要能够以MIB的形式统计过往包，记录在其路由器中，同样可以和计费服务器协同工作完成计费。

具体运行时，要想对一个校园网的所有IP地址进行计费，用于计费的路由器一定是位于整个校园网出口的。比如一般的校园网有一个出口连接到上一级节点，用于计费的出口路由器可以是连接上一级节点的路由器，也可以是与这一路由器具有单点连接的校园网路由器，而不是校园网内部的某个路由器。

计费工作的完成还需要计费服务器根据校园网的使用情况和出口路由器的性能情况，指定一定的时间间隔向出口路由器索取数据，完成计费。

采用标准网络管理协议SNMP进行IP流量统计曾是CERNET大多数IP计费系统采用的方法。这种方法的主要优点是：

1)原理简单。只采用网络管理常用的方法，只需要具备网络管理的基本知识即可。

2)对规模小的校园网适用。

它的主要缺点包括：

1)对网络带宽的性能影响很大。由于这种IP流量统计的方法是基于标准的SNMP协议，但SNMP协议的主要功能是完成异构网络的管理，协议的设计也主要从manager如何监视agent和如何接收agent的报告两方面来考虑。而利用这种方法进行IP流量统计需要由manager(计费服务器)每隔固定的时间间隔向agent(路由器)发出收集IP Accounting Table数据的SNMP请求。时间间隔的设定直接影响到manager向

作者简介：刘军良(1979－)，男，硕士研究生，主研方向：网络安全，网络管理；肖宗水，副教授
收稿日期：2007-12-13 **E-mail：**liujunliang@sdu.edu.cn

agent 发送命令的频繁程度。而时间间隔又是受校园网规模和出口路由器性能限制的。过于频繁的这类访问对校园网网络带宽的影响不容忽视。

2)对出口路由器的性能影响很大。在 SNMP 的 manager 和 agent 模型中，manager 每发送一次请求，要由 agent 予以响应，并根据请求的内容，应答相应的数据。IP 流量记录中由计费服务器发送给出口路由器的请求每次都需要路由器重复“ 响应－处理－发送 ”的过程，这大大加重了路由器的处理负担，降低了路由器的处理效率。

(2)利用 NETFLOW 的方法进行流量统计

NETFLOW 是 Cisco 公司为了提高网络效率采用的一种技术。网络上的流(network flow)是互联网上一对点之间的单向系列传输。“ 点 ”在这里由 IP 地址和传输层 PORT 识别，“ 单向系列传输 ” 是从一个 “ 点 ” 到另一个 “ 点 ” 的一系列连续传输。比如从某个 IP 地址的某个 PORT 发给另一个 IP 地址的某个 PORT 所有的连续传输称为一个 “ 流 ”。因此，利用 NETFLOW 技术进行流量统计只能在 Cisco 公司的路由器和带三层交换的交换机(NETFLOW 设备)上进行。

在 NETFLOW 的方法中，计费服务器配置专用软件，时刻监听。“ NETFLOW 设备 ”根据正常的工作，采用 NETFLOW 技术转发网络通信的同时，以流为单位记录对每个流的统计信息。待某个流的传输完毕后，把 NETFLOW cache 中对该流的统计信息一次性发送给计费服务器的监听进程。由计费服务器进行整理，生成 IP 流量统计，见图 1、图 2。

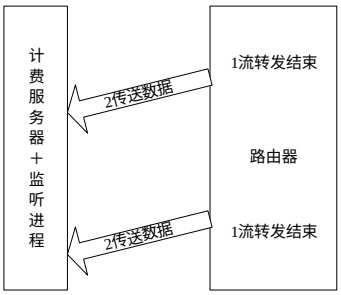

图 1　利用 NETFLOW 技术的流量统计

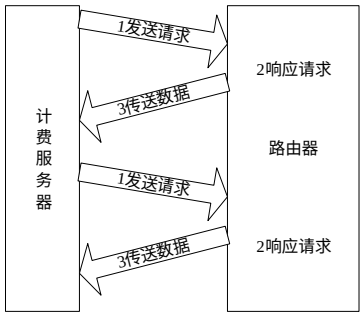

图 2　利用 SNMP 技术的流量统计

由图 1、图 2 可以看出，利用 NETFLOW 技术比 SNMP 方法统计流量更简便、效率更高，对网络带宽和网络设备性能影响较小。但这种方法存在设备局限性，仅能在 “ NETFLOW 设备 ” 上完成。

2　基于终端的分布式网络流量监测

如前所述，SNMP, NETFLOW 等流量监测方式存在很大局限性。而造成这些局限的重要原因是网络上所有流量统计的工作都由路由器和计费服务器完成，使这 2 个服务器不堪重负，性能下降，易造成网络效率瓶颈现象。本文提出基于终端的网络流量监测，这种新的流量监测方式把 IP 流量统计工作分解，使网络内所有的终端都参与流量监测工作，明显减少了服务器工作量，提高了网络整体性能。实现技术路线见图 3。

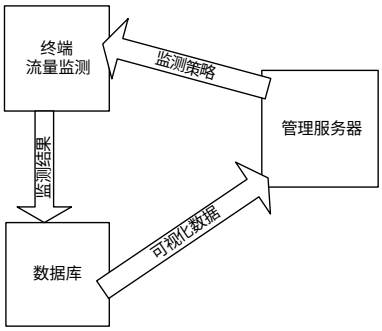

图 3　实现技术路线

图 3 中终端流量监测结果将该终端的网络流量统计结果发送到数据库；数据库的数据供管理服务器对网络整体性能进行分析；管理服务器控制终端流量监测的策略。

2.1　部署在终端的网络流量监测技术方法

部署在终端的客户端程序采用智能客户端技术，该客户端程序可以即用即下载、自动匹配版本、支持断点续传。因为只在后台与服务器系统交换所需的数据，所以让人感到它与其他系统交换的数据量减少。智能客户端已经基本做到零维护。

网络流量监测作为其功能模块采用 winpcap 技术实现。

(1)获取网络设备

函 数　int pcap_findalldevs_ex(char * source,struct pcap_rmtauth * auth,pcap_if_t ** alldevs,char * errbuf) 的作用是列出终端所有网卡，其中，pcap_if_t 是一个链表的节点：

```
struct pcap_if {
struct pcap_if *next;
char *name;
char *description;
struct pcap_addr *addresses;
u_int flags;
}
```

它将终端设备指针作为链表形式表示出来。

(2)打开网络设备

如果列出网络设备成功，下面利用函数 pcap_open()为捕获数据打开一个普通的源：

```
pcap_t *pcap_open(const char *      source,
int                         snaplen,
int                         flags,
int                         read_timeout,
struct pcap_rmtauth *       auth,
char *                      errbuf)
```

source：包含要打开的源名称的以’\0’结尾的字符串。源名称得包含新的源规范语法(Source Specification Syntax)，并且它不能为 NULL。为了方便地使用源语法，需要记住：1)pcap_findalldevs_ex()返回的适配器(网卡)可以直接被 pcap_open()使用；2)万一用户想传递他自己的源字符串给 pcap_open(), pcap_createsrcstr()，可以创建正确的源标识。

snaplen：需要保留的数据包的长度。对每一个过滤器接收到的数据包，第 1 个 “ snaplen ” 字节的内容将被保存到缓冲区，并且传递给用户程序。例如，snaplen 等于 100，那么

每一个数据包只有第 1 个 100 Byte 的内容被保存，即从每一个包的开头到 snaplen 的那段内容将被保存。

flags：保存一些由于抓包需要的标志。Winpcap 定义了 3 种标志：

1)PCAP_OPENFLAG_PROMISCUOUS：定义了适配器(网卡)是否进入混杂模式(promiscuous mode)。

2)PCAP_OPENFLAG_DATATX_UDP：定义了数据传输(假如是远程抓包)是否用 UDP 协议来处理。

3)PCAP_OPENFLAG_NOCAPTURE_RPCAP：定义了远程探测器是否捕获它自己产生的数据包。

read_timeout：以毫秒为单位。用于设置在遇到一个数据包时读操作不必立即返回，而是让更多的数据包到来后从 OS 内核一次读多个数据包。并非所有的平台都支持 read_timeout；在不支持 read timeout 的平台上它将被忽略。

auth：一个指向“ struct pcap_rmtauth ”的指针，保存一个用户登录到某个远程机器上时的必要信息。假如不是远程抓包，该指针被设置为 NULL。

errbuf：一个指向用户申请的缓冲区的指针，存放该函数出错时的错误信息。

返回值是一个“ pcap_t ”指针，它可以作为下一步调用(例如 pcap_compile())的参数，并且指定了一个已经打开的 winpcap 会话。在遇到问题的情况下，它返回 NULL 并且“ errbuf ”变量保存了错误信息。

(3)连续获取流量数据

统计流量需要连续不断地抓包，因此，winpcap 提供了函数 pcap_loop：

```
int pcap_loop( pcap_t*        p,
int            cnt,
pcap_handler   callback,
u_char*        user)
```

该函数会一直保持读数据包的操作直到 cnt 包被处理或者发生了错误。cnt 指明了返回之前要处理数据包的最大数目。如果 cnt 为负值，pcap_loop()将一直循环(直到发生错误才停止)。出错时返回－1；cnt 用完时返回 0；在任何包被处理前调用 pcap_breakloop()来中止循环将返回－2。

而上面函数参数之一 pcap_handler

```
hypedef void (* pcap_handler)(u_char* user,
const struct pcap_pkthdr* pkt_header,
const u_char* pkt_data)
```

用来接受数据。

至此，客户端最基本的流量监测功能已经实现。当管理服务器实施监测策略时，如离散时间监测、监测特定范围源地址流量，在 winpcap 技术基础上均可以很好地解决。

终端和数据库服务器采用 UDP 协议通信，客户端将按照管理服务器策略监测流量的数据主动发往数据库服务器。

2.2 数据库功能

数据库服务器提供一个 UDP 监听端口，用于接收来自客户端的流量统计报告，UDP 报文的内容包括报文类型(流量报文)、入流量、出流量、入报文个数、出报文个数。

数据库设计时必需的表见图 4、图 5。

字段	类型	大小	唯一	主键	说明
ID id			y		
MAC 地址 mac			y	y	
终端密码 password					
区域 area					
接入位置 location					填写具体的终端位置，例如房间号
接入时间					
IP 地址 ip					
终端所有人 owner					
联系电话 tel					

图 4 终端表

字段	类型	大小	唯一	主键	说明
ID id			y		
IP 地址 ip					
MAC 地址 mac					
入流量 input					
出流量 output					
入报文个数 inDatagram					
出报文个数 outDatagram					
最后更新时间 updatetime					

图 5 流量统计表

2.3 管理服务器功能

管理服务器主要具有如下功能：

(1)管理服务器由管理人员提供终端监测流量策略。

(2)根据数据库提供的数据计算分析网络整体情况以及各个终端网络情况。

(3)根据分析需要和分析结果重新改进监测策略，利用智能客户端优势，自动更新终端上客户端监测策略模块。

3 结束语

随着网络应用的不断拓展和网络技术的飞速进步，网络问题越来越复杂。而作为各种网络管理行为的基础，网络流量监测必须适应大流量、复杂的网络情况。由上述分布式网络流量监测技术方法可以了解，这种网络流量监测方法适用于方便统一管理的企业、单位和学校等网络环境。因为这种方法采用分工协作方式工作，分布式有利于任务在整个计算机系统上进行分配与优化，克服了传统集中式系统会导致中心主机资源紧张与响应瓶颈的缺陷，不存在性能瓶颈，所以不受限于网络规模的大小、网络带宽以及 IP 版本，可以适应较大规模的下一代高速网络。由于终端采用智能客户端技术，因此网络管理功能扩展性极强。利用智能客户端的特性，在对终端用户透明的情况下，可以根据流量监测情况对终端使用各种管理手段。

参考文献

[1] 陈 萍, 孙洁丽. IP 计费几种常用技术比较及对 IP 统计数据的进一步分析[J]. 计算机工程, 2000, 25(10): 35-37.

[2] 赵新元，王 能. 基于 Web 的网络流量监测系统的设计[J]. 计算机工程, 2007, 33(3): 237-239.