基于SNMP计算机网络流量监控系统研究

张 彤,吴世荣
(华北电力大学 数理学院,河北 保定 071003)

摘 要:针对一般网络流量监控商业软件普遍存在兼容性差,难于满足特定局域网络监控要求,网管人员很难有效监控网络的数据流走向、各个网络结点间的数据流状况及其他网络异常情况,并且软件价格昂贵。根据局域网线路数据流量测量和分析的实际需求,设计了基于SNMP的计算机网络流量监控系统通用方案,介绍了在VC++6.0平台下利用SNMP++技术和管理对象库MIB开发网络流量监控系统的过程,较好地解决了流量数据采样中遇到的技术问题。通过仿真测试,该系统所生成的流量图与MRTG生成的流量图基本一致,而且该系统实现简单、工作可靠稳定,可以作为开发局域网络监控系统软件的范例。

关键词:网络管理;流量监控;数据分析
中图分类号:TP393.02 **文献标识码**:A **文章编号**:1673-629X(2011)01-0088-04

Research on Computer Network Traffic Monitoring System Based on SNMP

ZHANG Tong, WU Shi-rong
(School of Mathematics and Physics, North China Electric Power University, Baoding 071003, China)

Abstract: The compatibility of general commercial software of network traffic monitoring is poor, hard to meet a specific local area network monitoring requirements. Network managers are very difficult to monitor effectively the network data flow direction, the state of data flow among every network node and other network abnormal. In addition, the software is expensive. In this paper, according to the actual requirement of the measurement and analysis of the local area network data traffic, design a universal program of network traffic monitoring system which is based on SNMP. The paper also detailed describes the development process of the network traffic monitoring system by using SNMP++ technology and Management Object Library MIB in the VC++6.0 platform. It solves well the technical problems in data sampling. By simulation testing, the traffic chart generated by this system is essentially same with the traffic chart generated by MRTG, the implementing process of this system is simple. Furthermore, system run is reliable and stable. This system can be used as an example of the software development of the local area network monitoring system.

Key words: network management; traffic monitoring; data analysis

0 引 言

进行流量监控和流量分析是整个网络管理的重要环节,网络流量监测提供了一种在实际环境中探索网络特性的手段。网络流量监测是一个从网络设备上采集数据、解码数据、分析数据的过程,它从网络中采集一些具体的指标性数据,反馈给监测者,这些数据为网络的运行和维护提供了重要信息,对于网络的资源分布、容量规划、网络性能分析、异常监测与隔离、安全管理等都是十分重要的。它能在最短的时间内发现安全威胁,在第一时间进行分析,通过流量分析来确定攻击,然后发出预警,快速采取措施[1]。近年来,许多学者对于网络流量监控以及网络安全管理等方面进行了较深入的研究,并取得许多有意义的结果。文献[2]引进了一种异常故障容错多阶段交互网络,用于并行处理大量的信息流,提高信息处理效率;文献[3]研究了基于着色Petri网的信息流安全模型,用于防止信息泄露;文献[4]给出了一种目录访问协议,为用户登录或检索数据进行认证。

开发计算机网络流量监控软件,比较传统的方法是利用MRTG这款监控网络流量负载软件进行二次开发,它是一个支持多个路由器的网络流量图形显示软件[5,6]。但利用MRTG软件开发有特殊要求的局域网络数据流量监控系统有一定的局限性。文中采用了

收稿日期:2010-05-12;**修回日期**:2010-08-10
基金项目:国家自然科学基金资助项目(50971059)
作者简介:张 彤(1959-),女,河北保定人,高级工程师,研究方向为计算机网络管理与信息处理技术;吴世荣,浙江台州广播电视总台工程师。

在Windows XP平台上利用VC++ 6.0语言进行开发，无需对现有网络结构进行改动即可运行，系统本身不加重网络的负荷，可适用于任何拓扑结构的网络,具有很好的移植性和灵活性。另外,在VC++6.0平台下,将SNMP++技术和管理对象库MIB很好地结合开发了网络流量监控系统,实现了设备扫描、数据采样、数据实时显示、流量图形显示和数据分析等模块功能。

1 SNMP工作原理

1.1 SNMP网络管理协议

简单网络管理协议[7,8](Simple Network Management Protocol,简称SNMP)已经成为事实上的标准网络管理协议。SNMP是由一系列协议和规范组成的,它提供了一种从网络设备中收集网络管理信息的方法。

SNMP的体系结构分为SNMP管理者(SNMP Manager)和SNMP代理者(SNMP Agent),每一个支持SNMP的网络设备中都包含一个代理,此代理随时记录网络设备的各种情况,网络管理程序通过SNMP通信协议查询或修改代理所记录的信息。

在使用TCP/IP协议的互联网环境中,管理协议标准是SNMP,它定义了传送管理信息的协议消息格式及管理站和设备代理相互之间进行消息传送的规程。

1.2 SNMP工作原理

SNMP网络管理系统主要由管理者、代理和被管理者三个基本组件构成[9]。管理者通常是网络中的一台安装网络管理软件的工作站或服务器;代理是驻留在被管理设备上的一个模块,通过SNMP协议与管理者进行通信。管理者按一定时间间隔向各个设备的代理发送查询请求管理信息,并根据管理信息来跟踪各个设备的状态,判断是否有异常事件发生。当管理对象即设备出现发生紧急情况时,设备代理可以使用Trap信息的报文主动向管理者发送陷阱消息,汇报出现的异常事件。这些轮询消息和陷阱消息的发送和接受规程及其格式定义都是由SNMP协议定义的;被管理设备将其各种管理对象的信息都存放在管理信息库(Management Information Base)[10,11]中。

2 基于SNMP++的Windows环境下SNMP编程技术

在文中,SNMP管理技术的实现主要采用SNMP++技术[12,13]。该技术把WinSNMP API函数等核心部分面向对象封装成相关的C++类。开发关键步骤主要有两点:①构造并组建正确的用户数据报协议(UDP)和SNMP报文;②对发送或接收的SNMP报文进行BER编码解码。

将BER编码处理后的SNMP报文提交给用户数据报协议,并指定工作站或服务器端(SNMP代理)IP地址和端口号即可;当接收到返回的应答信息包后,再对SNMP报文进行解码处理、分析。

3 计算机网络流量监控系统的总体设计与实现

3.1 总体设计方案

测量网络流量首先要获取网络设备接口流量的原始数据;然后按一定的时间间隔连续地取出设备中接口的相关SNMP变量的值;最后将获取的结果以图形方式显示在屏幕上,并将数据以文本文件形式保存或存到数据库中,以便进一步分析、处理。

3.2 系统开发环境

系统开发环境:采用Visual C++6.0,基于SNMP++包。

3.3 程序实现

3.3.1 模块设计

系统包括设备扫描模块、数据采样模块、数据实时显示模块和数据分析模块。

3.3.2 设备扫描模块

首先要对给定的设备进行系统扫描,然后将设备中所有物理接口的相关信息取回并显示。这里要用到OID,如表1所示。

表1　设备扫描模块使用的OID

OID	描述
1.3.6.1.2.1.2.2.1.1	接口索引
1.3.6.1.2.1.2.2.1.2	接口名称
1.3.6.1.2.1.2.2.1.8	接口工作状态
1.3.6.1.2.1.2.2.1.5	接口最大速率
1.3.6.1.2.1.4.20.1.2	接口IP地址
1.3.6.1.2.1.31.1.1.1.18	备注

3.3.3 流量数据采样模块

流量数据采样模块是从网络设备接口中读取流量数据并进行计算。取回的数据是设备接口在某一时刻发送或接收的累计信息流总字节数,因此,需要计算出两次数据之间的差值,并由字节数换算成位,再除以时间间隔(以秒为单位),就可得到这段时间内的平均流量。

在编写程序时需要注意下面四个问题:

(1)选择适合的数据类型。

MIB规定计数器是Counter类型,且为四字节无符号整数,其取值范围是0~4 294 967 295。而C++中的

int 类型为带符号位的四字节整数，因此不能用它来存储读取数据，需要使用 unsigned int 类型。Int 类型的长度由实际设备的操作系统和编译系统而定。

(2)确定采样时间间隔。

从理论上讲采样时间间隔越小，取到的数据越多，得到结果也越准确。但实际上并不是取样时间间隔越小越好，频繁的读取数据操作会影响网络设备的性能，同时还会产生更多的网络流量。因此，本文采样时间间隔定为 5 分钟。

(3)除数的选择。

网络系统繁忙时产生的延时会影响数据的准确性，因此在读取流量数据的同时，应注意读取网络设备的系统时间，并将两次获得的流量数据差值除以时间差值。

(4)计数器归零问题。

监测系统计数器达到最大值时，计数器会从零重新累加计数，那么流量数据计算结果一定是一个负数，应该避免这种情况出现。在网络带宽比较低的情况下，这种问题较少遇到。但在高带宽的情况下，就要考虑在程序中加以处理。处理方法是将每次读取的数据与上次的数据相比较，若小于上次的数据，说明出现了计数器归零的问题，此时应该将得到的结果再加上 4 294 967 295。

表 2 是带宽不同的情况下，计数器从 0 开始计数，达到最大值归零所需的大概时间。

表 2 带宽与计数器归零的时间关系

带宽	计数器归零时间(分)
1Mbps	546.1
10Mbps	54.61
100 Mbps	5.46
155 Mbps	3.52
1Gbps	0.55

3.3.4 流量数据实时显示模块

流量数据实时显示模块功能是将取回的信息流经计算后得到的数据实时地用图表显示出来，动态地显示流量数据曲线。其中两根曲线分别表示一条线路上的输入、输出数据。

根据系统的需要，该模块应有如下的特点：

①有一个对应的窗口，以方便我们在上面画曲线图；

②能接收输入的数据，并将这些数据以图形方式按比例显示出来；

③显示的图形能够左右移动，以显示更多的数据；

④在显示新输入数据的时候，以前显示的数据也不消失，要同时显示；

⑤带有坐标系，横坐标表示时间，纵坐标表示数据；

⑥横坐标的标注显示能够调整，以避免过多的显示使标注相互叠加，模糊不清；

⑦纵坐标刻度值能够根据显示数据的最大值自动调整到一个合适的值，而不应该固定不变。

根据本程序的特点，一个时间点对应显示的数据有流出、流入的数据，还要保存此时的流出利用率、流入利用率等数据。这些数据被存放到一个结构类型的变量中，所有被显示的数据存放在以该种结构类型数据为元素的一个数组中。

采样数据时间间隔为 5 分钟，为能显示一天时间采集的数据，横轴显示数据区为 12×24 = 288 个显示位置。数组大小也为 288 个元素，以保存这些数据。当数据多于 288 个时，以前的数据被依次丢弃，只显示、保存最新的 288 个数据。

新添加的数据显示在曲线的最右边，以前显示的数据依次向左移动一个显示位置。为使曲线看起来更流畅，横坐标一个显示位置定为屏幕坐标的一个像素。横轴每隔 36 个显示位置显示一下时间标记。

图形中有两条曲线，第一条曲线采用根据数组中的数据，计算出该数据在坐标系中的位置，然后将相邻的点连接起来，形成一条曲线；另外一条曲线采用从数据点向横轴画直线的方式，因为一个显示位置在屏幕上是一个像素坐标，因此看起来的效果是被填充覆盖区域的曲线。

3.3.5 数据分析模块

网络流量测量结束后，还要对取回的数据进行分析。主要是通过观察流量曲线有无异常，流量数据的最大、最小值，平均流量数据有多大以及某一时刻的数据流量有多大等几方面进行分析，并通过与流量历史数据对比来判断当前网络是否安全、可靠、正常，为提供一个具有全网动态实时监测与自校正能力的拓扑的优化设计与管理方案奠定基础。

数据分析状态时，控件中的数据从一个数据文件中读入。当数据个数超过显示数据数组大小时，增加数组中的元素个数以保存更多的数据。分析数据时，随鼠标的移动，在显示区画十字线，同时显示鼠标所在位置数据的最大值、最小值等数据。同时还可以向左右移动。

4 系统调试与仿真结果分析

4.1 程序主界面

程序主界面如图 1 所示，程序在初始化时随机生成一个日流量图和周流量图。

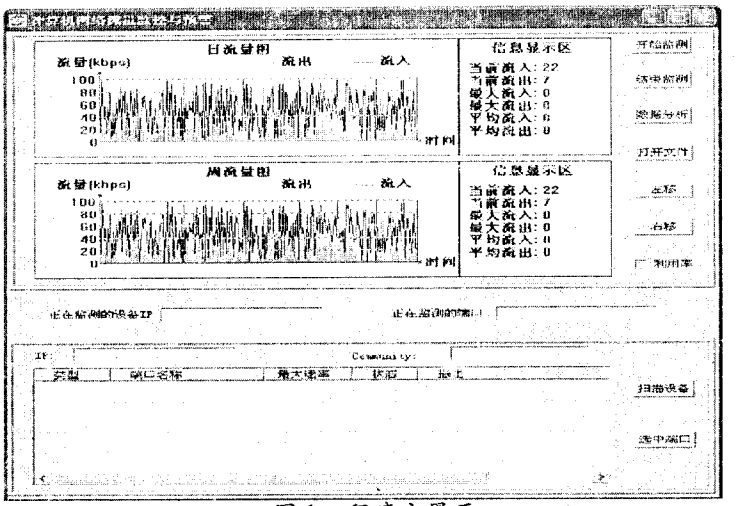

图 1　程序主界面

4.2　本系统与 MRTG 生成的流量图对比

用本程序生成的流量图,如图 2 所示。

MRTG 生成的流量图,如图 3 所示。

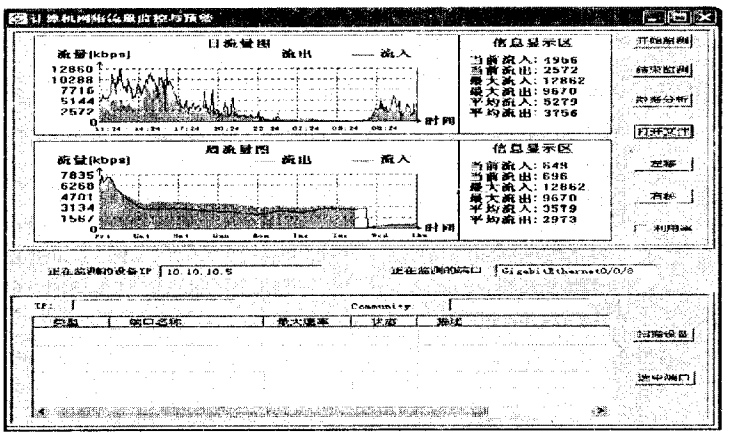

图 2　本程序生成的流量图

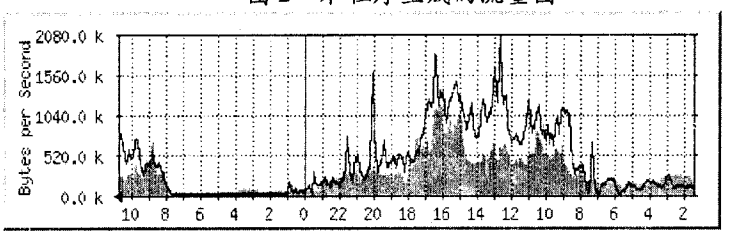

图 3　MRTG 生成的流量图

MRTG 生成的流量图最新的数据显示在左边,本程序的最新数据显示在右边。如果将图 3 水平翻转,再与图 2 比较,容易看出:两个程序的监测结果图形是十分相似的。然而,因为两个程序启动时间不同,使得它们采样的时间段不同,因此所生成流量图并不完全一致。显然,线路上的流量越大、越不均匀,不同时间段采样得到的结果相差越大。

5　结束语

该软件在华为交换机和路由器测试通过,从理论上讲能够对任何支持 SNMP 协议的网络设备进行流量监控。

为简单起见,所编制的程序在同一时间只能对一台设备的一个物理端口进行监控,如果要对核心交换机以及下联的接入交换机的每个端口进行监控,即同时监控整个网络的多个端口,还需要对程序在多线程监控方向做些修改。本论文将理论和实践进行了很好的结合。

参考文献:

[1]　杨晓宇. 浅谈企业网络管理的重要性[J]. 油气田地面工程,2005,24(11):57-57.

[2]　Sharma S, Bansal P K, Kahlon K S. On a class of Multitistage Interconnection Network in Parallel Processing[J]. International Journal of Computer Science and Network Security, 2008(5):287-291.

[3]　Wu Ruoyu, Li Weiguo, Huang He. Colored Petri Nets Based Modeling of Information Flow Security [C]//Proceedings of Second International workshop on Knowledge Discovery and Data Mining. Moscow, Russia:[s. n.],2009:681-684.

[4]　Salim M, Akhtar M S, Qadeer M A. Data Retrieval and Security using Lightweight Directory Access Protocol[C]//Proceedings of Second International workshop on Knowledge Discovery and Data Mining. Moscow, Russia:[s. n.],2009:685-688.

[5]　赵　英,黄九梅,董小国,等. 网络流量监控系统的设计与实现[J]. 计算机应用,2004,24(S1):32-33.

[6]　赵永胜. MRTG 在网络管理中的应用[J]. 铁路通信信号工程技术,2005(12):43-45.

[7]　IETF. Simple Network Management Protocol (SNMP) [S/OL]. [2007-06-01]. http://www.faqs.org/rfcs/rfc1157.html.

[8]　IETF. Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2) [S/OL]. [2007-06-01]. http://www.faqs.org/rfcs/rfc1902.html.

[9]　田增国,刘晶晶,张召贤. 组网技术与网络管理[M]. 北京:清华大学出版社,2009.

[10]　李　霞. 简单网络管理协议及其实现方法的比较[J]. 淮阴工学院学报,2005,14(1):54-55.

[11]　高　阳,王坚强. 计算机网络原理与实用技术[M]. 北京:清华大学出版社,2009.

[12]　吴昊,杨　凯,胡　术,等. SNMP 跨平台移植和交换机端口 IP 探测[J]. 计算机技术与发展,2008,18(11):18-21.

[13]　蔡　琳. 在 VC++6.0 平台下基于 SNMP 网络管理软件的开发[J]. 信息与电子工程,2005,3(3):224-227.