基于 SNMP 的校园网管理系统的设计与实现 *

何 鹏

(中原工学院,河南 郑州 450007)

摘 要:介绍了一个适合于校园网的基于 SNMP 的网络管理系统的设计与实现。以管理者/代理为模型,采用分层次的总体设计方案。在分析比较现有拓扑发现算法的基础上,给出一种改进的拓扑发现算法,融合二叉树排序策略和三层交换机发现策略。在实时性能参数采集分析的基础上,结合概率论与数理统计的思想,建立了一元线性回归模型,对性能参数进行有效的区间预测。系统不仅设计了网络的拓扑结构发现及显示、配置管理、性能管理等核心功能,更针对性地设计了网络性能预测、流量排序、病毒及非法软件检测等功能。

关键词:简单网络管理协议;管理信息库;拓扑结构;配置管理;性能管理

中图分类号:TP393.07 文献标识码:A 文章编号:1674-7720(2010)17-0053-04

Design and implementation of network management system for campus based on SNMP

HE Peng

(Zhongyuan University of Technology, Zhengzhou 450007, China)

Abstract: This paper describes the design and implementation of a network management system based on SNMP, which is suited for campuses. The system takes manager/agent models and use hierarchical design program. After analyzing the existing topology discovery algorithm, the paper proposes an improved topology discovery algorithm, which integrates strategies of binary sort tree and 3-layer switches discovery. In order to execute effective range forecast, the paper establishes a linear regression model integrating mathematical statistics theory, on the basis of real-time acquisition and analysis to performance parameters. The system not only designs the network topology discovery and display, configuration management, performance management and other core functionality, but also designs the network performance prediction, flow sorting, viruses and illegal software testing capabilities more targeted.

Key words: SNMP; MIB; topology structure; configuration management; performance management

目前市面上有很多商品化网管软件,如 IBM 公司的 NetView、HP 公司的 OpenView、SUN 公司的 Sun NetManager 等,这些网络管理软件尽管功能很强大,但提供的是一个通用的网络管理平台,对于具体校园网管理应用,还得进行进一步的规划和开发。因此,迫切需要开发一个适用于高校校园网的网络管理系统对日常的网络设备和网络运行情况进行监督与维护。

1 系统总体设计

本网络管理系统的总体设计目标就是要构建一个基于 SNMP 的多代理的统一管理、简便直观、兼容不同厂商设备、能够实现网络拓扑结构发现、配置管理、性能管理等功能,并针对校园网上机特点,实现对所有运行主机的管理。具体内容如下:

(1)网络拓扑结构发现

找出路由器与路由器、路由器与子网之间的连接关系,并发现所有子网中活动的 IP 设备,区分出路由器、交换机和普通主机。对网络拓扑发现结果进行图形化显示。

(2)配置管理

本系统的配置管理主要实现路由器(或三层交换机)的配置管理和主机的配置管理。路由器配置管理具体包

* 基金项目:河南省科技攻关基金资助项目(092102310038,092102210029)

括获取路由器的常规配置参数(如设备类型、负责人、支持服务、所在位置等),获取路由表信息、地址表信息、地址转发表信息、接口表信息以及接口状态表信息等。主机配置管理包括查看主机的基本信息、安装软件信息、运行软件信息、存储器信息、硬件设备信息等主机资源信息。

(3)性能管理

对代理设备的原始性能数据进行实时采集。对采集到的性能数据进行分析,计算接口流量、协议流量等各种性能参数,为管理员提供参考。

查询某一时段代理设备的性能参数,生成性能曲线,以直观图的方式显示性能分析结果。

根据某一时段代理设备的性能分析结果,对网络性能进行分析预测,并以直观图的形式显示出来,为网络管理员采取进一步措施提供依据。

(4)流量排序

流量排序分为接口流量排序和主机流量排序。接口流量排序是对网络中所有发现的接口进行流量采集并排序,将结果以直观图的形式显示出来,供管理员查看。主机流量排序对网络中某一子网内所有主机流量进行实时采集并排序,将结果以直观图的形式显示出来,供管理员查看。

(5)病毒及非法软件检测

对网络中某一子网内所有主机进行病毒或非法软件排查工作,找出该子网内所有运行指定软件名称的主机,并将结果以直观图的形式显示出来,供管理员查看。

2 系统模型结构

本网络管理系统以SNMP网络管理协议的管理者/代理模型为基础[1],以HP公司的SNMP++为数据采集工具,采用分层的方法,面向系统的不同功能设计而成。

该系统分为三个部分如图1所示:底层数据通信、中间层数据处理与上层数据表示。底层数据通信部分负责实现管理者与被管设备之间的通信,获取代理设备中MIB库的有用信息,并把采集到的数据送往上层。中间层数据处理部分负责对采集到的网络信息进行处理,将

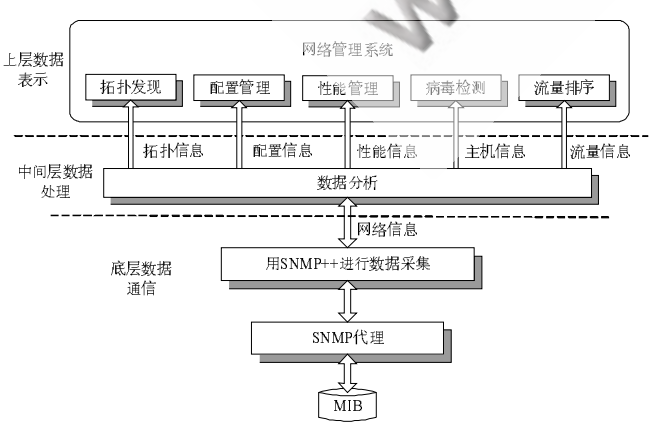

图1 系统设计框架的分层逻辑结构

相应的处理结果传给上层管理应用层进行显示。上层为数据表示层,对网络的配置管理、性能管理等功能模块以表格和可视化的图形界面显示,简洁直观。

3 系统关键技术分析

3.1 网络拓扑结构发现算法的研究与分析

基于SNMP协议的算法实际上是提取MIB中ipRouteTable(路由表)中的对象,类似于图论中的广度优先遍历算法实现网络拓扑的自动搜索[2]。

设计路由发现算法时主要用到了三条链表:待检路由设备链表、拓扑信息链表、子网信息链表。基于SNMP的拓扑发现算法通常是使用一个种子路由器,获取其路由表内记录的所有可达网段,以及到达该网段所经由的下一跳路由器的端口IP地址及相关路由信息,然后将继续扩展其搜索,一直达到用户指定的深度为止。同时种子路由器还可以获取到每个路由设备上所有端口的直连子网及其相应的子网掩码,根据这些信息,进而获取到这些子网中的所有活动主机。如果这些设备支持SNMP,则还可以进一步收集系统和IP地址信息。总之,只要给出一个路由设备任意端口的IP地址作为种子路由器(通常使用本地网关的IP地址作为种子路由器的地址),即可获取到指定深度内的所有路由设备及活动主机的网络拓扑结构信息。

(1)默认网关的获取

拓扑发现算法首先是从网络管理站的默认网关开始,逐步遍历默认网关的路由表和地址解析表,最终发现整个网络的拓扑结构。本系统获取默认网关是采取这样的方法:首先,访问拓扑发现程序所在计算机的SNMP MIB中的ipRouteTable,如果发现有ipRouteDest值为0.0.0.0的记录,则说明程序所在的计算机设置了默认网关,该记录的ipRouteNextHop值即为默认网关的地址。检查默认网关的ipForwarding值,如果为1,则表明该默认网关确实是路由设备,否则不是。

(2)设备类型判断

利用SNMP协议,提取MIB中的$sys_{services}$对象实例值,然后根据返回的值判断类型。如果目的设备不返回SNMP响应报文或响应超时,则认为设备没有配置SNMP,类型为一般工作站。

对于路由设备的判定,一般是通过MIB库中的system组中的$sys_{services}$值来判定的。如果设备的第i层提供了服务,则L_i被赋予相应的层数:$sys_{services}=\sum_{(i=1)}^{L_i}2^{(L_i-1)}$。

在区分交换机和其他主机时,可根据$sys_{service}$变量和IpForwarding变量。$sys_{service}$变量的值可以确定设备工作在第几层,IpForwarding确定设备是否具有转发功能,如果IpForwarding不为1,且$sys_{service}$为1,则Device为交换机,如果不能获取到$sys_{service}$和IpForwarding变量,或者IpForwarding和$sys_{service}$是其他组合,则为一般主机。

(3)路由器多 IP 地址问题

由于路由器可以连接多个子网,具有多个接口,即一个路由器可能含有多个 IP 地址。为了准确标识具有多个接口的路由器,避免重复,本算法通过访问路由器的地址表获得路由器的所有接口,这样可以根据当前路由器的 IP 是否在已经遍历过的路由器接口列表中来判断。

3.2 性能预测模块的设计

本模块根据一元回归模型的数学原理,找出网络流量与时间之间的关系,建立一元线性回归方程:$\hat{Y}=\hat{a}+\hat{b}x$。

其中,$\hat{a}=\bar{Y}-\hat{b}\bar{x}$,$\hat{b}=\dfrac{\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{\sum_{i=1}^{n}(x_i-\bar{x})^2}$。

对于给定的置信度 $1-\alpha$,在 $x=x_0$ 处的置信区间为:$\{\hat{Y}_0+\delta(x_0),\hat{Y}_0+\delta(x_0)\}$。其中,$\delta(x_0)=t_{a/1}(n-2)\hat{\sigma}\sqrt{1+\dfrac{1}{n}+\dfrac{(x_0-\bar{x})^2}{\sum_{i=1}^{n}(x_i-\bar{x})^2}}$。$\sigma^2$ 的无偏估计为 $\sigma^2=\dfrac{Q_e}{n-2}$,而 $Q_e=\sum_{i=1}^{n}(y_i-\hat{y})^2-2\hat{b}\sum_{i=1}^{n}(x_i-\hat{x})^2(y_i-\hat{y})^2+\hat{b}^2\sum_{i=1}^{n}(x_i-\hat{x})^2$。

本系统默认预测分析算法的置信度为 $1-\alpha=0.95$,在性能参数采集分析结果的基础上对性能参数的变化趋势进行预测。

图 2 是该模块的性能预测流程图。

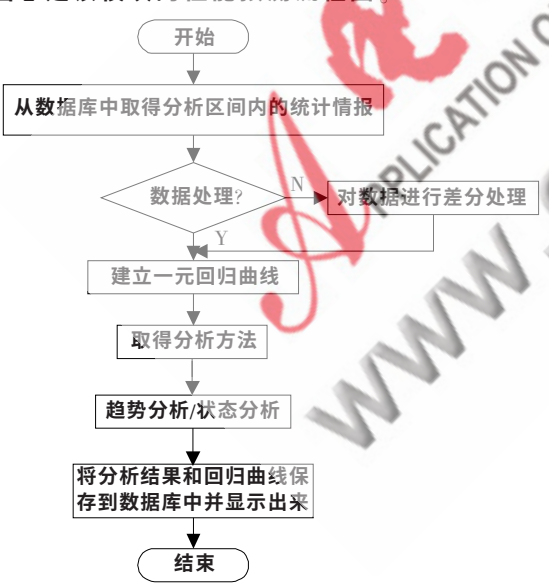

图 2 性能预测流程图

图 2 中,数据差分处理主要是有一些变量是逐渐增加的(如某接口的流出字节数),而系统关心的是两次流出字节数的差值,数据处理就是算出差值。趋势分析主要是计算出分析期间内的一元回归直线,以便在用户界面上显示出来时,网络管理者很容易看出它的增减趋势。而状态分析主要是将系统关心的一些变量的状态分析出来并报告给网络管理系统,以便系统根据变量的当前状态及时对其作出调整。

3.3 病毒及非法软件检测模块的设计

本系统中主机感染病毒或运行非法软件功能的实现是在拓扑发现结果的基础上,对管理员指定子网内的所有主机进行运行软件数据采集,将各主机中正在运行的软件名称和管理员指定的软件名称进行对比,最终排查出该子网内具体有哪些主机运行了指定的软件,并将排查结果存入相应的数据结构中,以直观图的形式显示出来。具体流程图如图 3 所示。

图 3 病毒及非法软件检测流程图

4 系统性能测试[3]

4.1 流量分析功能测试

本系统对网络中指定路由器各性能参数进行实时采集分析,将分析结果以曲线图的形式显示出来,如图 4 所示。图 4 中,细线表示接口入流量速率,粗线表示接口出流量速率。与同类产品(如华为 Quideway)比较,发现该流量实时采集模块采集分析结果与成熟网管软件分析结果无实质性差别,能够及时给网管人员提供有效信息数据,该模块具有正确性和可用性。

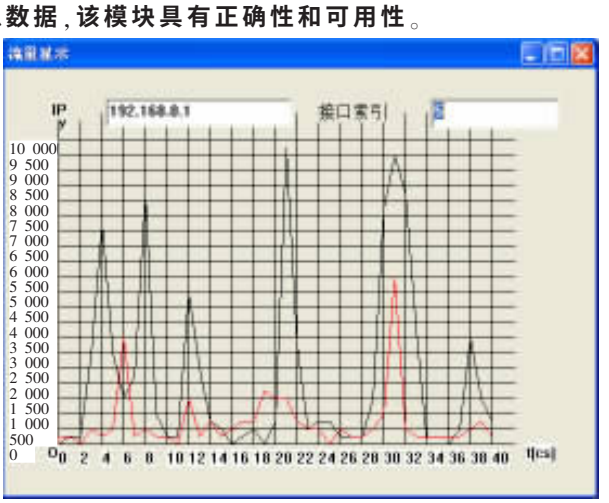

图 4 接口流量显示界面

4.2 流量预测功能测试

在流量采集分析的基础上运行系统性能预测功能，结果如图5所示。该部分流量预测模块是在图4接口流量采集分析基础上，利用了一元线性回归模型和区间预测算法，计算分析将来某一时刻接口的可能流量范围和流量发展趋势。本系统默认该预测分析算法的置信度为$1-\alpha=0.95$，系统流量预测结果与运用数学工具计算分析结果相吻合，系统具有正确性。

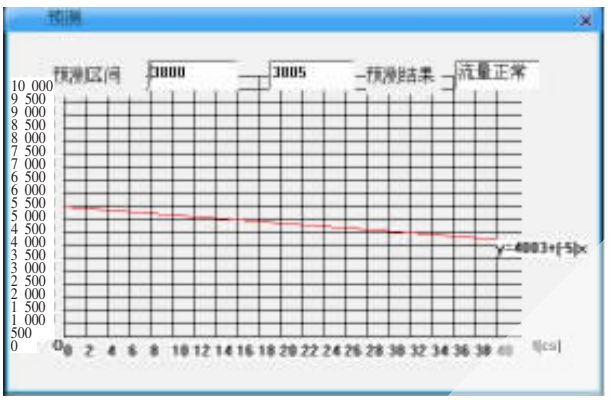

图5 预测分析界面和一元线性回归模型图

通过本系统在某高校试运行，结果显示该部分预测分析功能模块能够帮助网络管理员采用数学分析方法对网络流量进行及时预测，进而使得网络管理人员可及时发现网络问题并采取进一步措施，取得理想效果，该模块功能具有实用性和可靠性。

4.3 主机运行非法软件及感染病毒模块性能测试

运行该部分功能对指定子网内所有主机运行QQ应用程序进行排查，系统运行结果如图6所示。

通过具体的实地调查发现，该子网内所有用户在该时刻运行主机应用软件情况与系统运行结果完全吻合，由此可见该系统具有正确性和有效性。本部分功能模块有助于网络管理员限制某些对网络流量产生破坏的非法软件或病毒运行，将子网内运行非法软件或病毒的所有主机排查出来，网络管理员可根据具体情况对这些主机用户进行警告等处理。

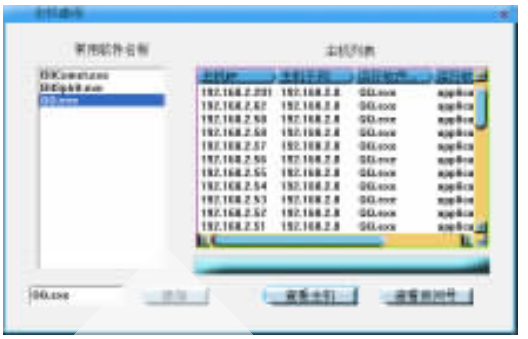

图6 运行QQ的所有主机显示界面

本文深入地分析了SNMP简单网络管理协议，结合校园网网络管理需求的特点，设计并实现了一个基于SNMP的网络管理系统。在本系统的设计与研究过程中，系统性分析了SNMP协议的原理、网络管理的关键技术以及拓扑发现算法，给出了一种融合二叉排序树策略和三层交换机发现策略的拓扑发现算法，能够发现网络中三层交换机和子网内所有主机，并对拓扑发现的结果进行图形化显示。在网络拓扑发现结果的基础上，进一步设计并实现了配置管理、性能管理、流量排序、病毒及非法软件检测等功能模块。该网络管理系统已经在北航计算机学院教学实验中心试运行并取得了较好的效果。

参考文献

[1] MARK A, MILLER P E. Managing internetwords with SNMP[M]. 北京:中国水利水电出版社,2001.

[2] CASE J, HARRINGTON D. Message processing and dispatching for the simple network management protocol, RFC2272[S]. January, 1998:82-135.

[3] ANALUCIA S M, LIUZ F K, CARLOS B W. Performance evaluation for proactive network management [J]. ICC, 2006 (6):22-36.

(收稿日期:2010-04-02)

作者简介:

何鹏,女,1983年生,硕士,讲师,主要研究方向:网络管理。