流量监测 MRTG 的改进及其实现*

蒋　海, 刘淑芬
(吉林大学 计算机科学与技术学院, 吉林 长春 130012)

摘　要: 介绍了目前被广泛应用的流量监测工具 MRTG 的实现机制, 指出它在大型网络流量监测中性能方面的严重不足, 提出了一种改进方法及其实现, 并结合应用实例展示了改进后的 MRTG 在性能上的显著提高, 对于相关软件的开发和应用具有一定的借鉴作用。

关键词: 流量监测; MRTG; 网络管理
中图法分类号: TP393　　**文献标识码**: A　　**文章编号**: 1001-3695(2006)02-0201-02

Improvement and Implementation of MRTG for Traffic Monitoring

JIANG Hai, LIU Shu-fen
(College of Computer Science & Technology, Jilin University, Changchun Jilin 130012, China)

Abstract: The mechanism of MRTG is introduced, and the disadvantages of MRTG in performance are indicated. The scheme of improvement is given. With experiment, the great performance improvement of improved MRTG is showed. It's also helpful to development and application of similar software.

Key words: Traffic Monitoring; MRTG; Network Management

流量监测对于网络管理有着重要意义, 是网络管理系统中一个主要的部分, 它可以反映网络的负载情况, 也可作为网络规划和排除网络故障的依据。MRTG (Multi Router Traffic Grapher) 是一个典型的流量监测工具[1], 由于具有良好的可移植性、可扩展性和图形化界面, 同时还是开放源代码的免费软件, 因此在国际范围内得到了非常广泛的应用。本文首先介绍 SNMP 协议和 MRTG 的工作原理与实现机制, 然后分析了 MRTG 在大型网络流量监测中存在的不足之处, 并针对这些不足给出一种改进方法及其实现, 最后结合我们的应用实例展示了改进后的 MRTG 在性能上的显著提高。

1　SNMP

SNMP(Simple Network Management Protocol, 简单网络管理协议) 是当今网络管理协议[2]的事实标准, 提供了从网络设备获取状态信息以及网络设备报告故障和错误消息的机制, 定义了网络状态、管理信息交换的框架。其中有两种实体, 即管理站(Manager) 和代理(Agent)。管理站负责与一个或多个代理进行通信, 查询各种状态变量的取值; 代理从网络设备获取管理信息, 每一个代理都有一个 MIB(Management Information Base, 管理对象信息库) 及一些与具体设备有关的变量。MIB 变量采用了符合 ASN.1 规范的对象标志方法 OID(Object Identifier), 用来唯一标志网络所需管理的对象或对象组。SNMP 主要操作有 SET, GET, GETNEXT, TRAP 等。体系结构如图 1 所示。

收稿日期: 2004-11-05; 修返日期: 2005-03-22
基金项目: 国家科技攻关项目(2004BA907A20)

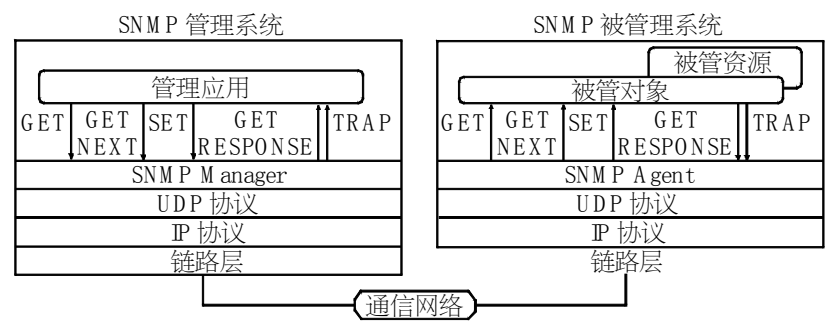

图 1　SNMP 体系结构

2　MRTG 的工作原理

MRTG[3~5] 主要有四个功能模块: SNMP 模块、日志文件、RateUp 模块、配置模块。

(1) SNMP 模块。为了增加系统的可移植性, MRTG-2 采用了 SIMON LEINN 的 PERL SNMP。PERL SNMP 完全用 PERL 语言写成, 可以独立于所运行平台。该模块以 SNMP 协议为基础, 通过与网络设备的 SNMP Agent 通信, 用 SNMP GET 操作获取需要的状态信息。在本文中主要是获取流量计数值 ifInOctects 和 ifOutOctects, 对应的 OID 标志为 1.3.6.1.2.1.2.2.1.10.x 和 1.3.6.1.2.1.2.2.1.16.x。其中 x 表示端口索引 Index 值。

(2) 日志文件。MRTG 使用日志文件以 ASCII 文本形式来记录测得的流量数据, 日志文件由 RateUp 模块进行更新。为了避免长期监测时数据膨胀问题, MRTG 定期对数据进行整合, 根据记录数据的日期不同而以不同的粒度保存数据, 随着时间的推移, 相应数据的粒度逐渐变大, 超过两年的数据不再保存。因此日志文件具有常量大小的特征, 能够支持长期的网络监测任务。

(3) RateUp 模块。在该模块中, MRTG-2 使用 C 语言程序来完成日志文件的更新和统计图形的生成, 与原来用 PERL 实现相比, 大大提高了效率。

(4) 配置模块。MRTG 提供了生成配置文件的工具。配置文件用于定义数据采集和图形定制时所需要的参数和规则, 它是扩展名为 CFG 的纯文本形式, 因此可以根据需要按照其规则进行修改。

MRTG 从配置文件(可以用配置模块生成, 也可人为生成) 中读取用于采集和个性化图形显示的配置信息, 调用 SNMP 模块从网络设备上获取原始数据, 接着调用 RateUp 模块处理日志文件, 并进行画图和生成 HTML 文件。其主要流程如图 2 所示。

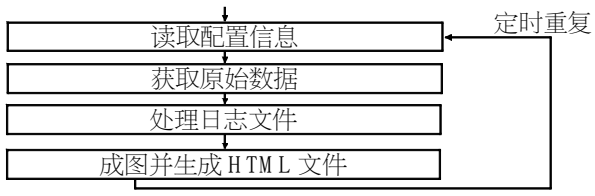

图 2 改进前 MRTG 工作机制

3 MRTG 的不足及其改进方案

在大型网络中, 需要进行流量监测的端口(包括物理端口和逻辑端口) 非常多, 通常数目都是在几千甚至几万个以上。MRTG 每次从设备采集数据并生成日志文件后, 接着进行画图, 尽管画图部分模块是用效率较高的 C 语言程序实现, 但它依旧是 MRTG 在性能上的瓶颈, 特别是当需要监测的端口数目急剧增多时, 导致不能在规定的周期(如 5min) 内执行完毕; 同时, 每个周期都对每个端口生成了流量统计分析图形, 而在实际应用场合, 一个端口的流量统计分析图形被用户调用查看的概率远远小于不被调用的概率, 因此白白浪费了大量的系统开销。

针对 MRTG 存在的上述性能方面严重不足, 我们引入了触发控制方式的 "即时成图", 具体工作流程如图 3 所示。改进后的 MRTG 在从设备获取数据方面与改进前没有区别, 但它在每个周期内只将获取到的数据处理后存储在日志文件中, 并不立刻生成流量统计分析图形。用户查看图形时, 需要触发成图控制模块, 成图控制模块会调用画图模块进行图形生成, 这时用户可查看到新生成的流量统计分析图形。

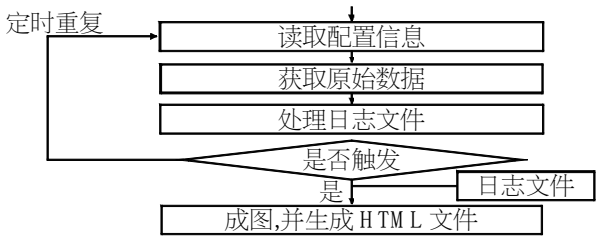

图 3 改进后的 MRTG 工作机制

4 应用实例

在对某市城域网一千三百多台设备(包括路由器和交换机) 进行流量监测时, 需要监测的端口数目大约是七千二百个。原 MRTG 在性能上不能满足应用的需要。在具体改进实现中, 采用了触发控制的方式, 对 MRTG 的源程序也进行了相应的修改。触发控制是使用控制报文来实现的, 控制报文是基于 TCP(传输控制协议) 的消息定义。SNMP 模块依然周期性地从设备上获取状态变量值, 处理后存储在日志文件中, 但不再更新原来的图形。当客户端需要查看某统计分析图形时, 首先向成图控制模块发送控制报文, 报文中指出了要调用哪个设备及端口的图形, 成图控制模块收到控制报文后根据日志文件进行类似原 MRTG 中的图形生成, 生成图形完毕后向客户端发送控制反馈报文, 客户端收到控制反馈报文后, 即可调用新生成的流量分析统计图。如果客户端在等待反馈报文时超时, 则重新发送控制报文。

在实例测试中, MRTG 改进前后的性能参数如表 1 所示。由表中数据我们可以看出, 尽管改进后的 MRTG 在客户端响应上有了一定的延迟, 但它大大减小了系统的开销, 缩短了执行时间, 使得流量监测最小执行周期可以显著缩小。其中, 硬件环境为主频 900MHz 的 CPU 两个, 内存大小为 2GB; 软件环境为 HP-UNIX 操作系统, MRTG 2.10.5, Perl 5.8.2。

表 1 改进前后性能参数表

改进时间	端口数	配置文件数	Forks 值	最小执行周期(s)	客户端响应时延(s)
改进前	500	2	5	40	<1
	2 000	8	5	150	<1
	7 000	28	5	950	<1
改进后	500	2	5	30	2 ~7
	2 000	8	5	80	2 ~7
	7 000	28	5	250	2 ~7

4 结束语

作为典型的流量监测工具, MRTG 还可以用于其他设备状态信息监测, 如 CPU、内存利用情况、其他流量信息等。改进后 MRTG 性能上得到显著提高, 克服了原来在大型网络流量监测方面的严重不足。在实际开发应用中, 这种改进方案也取得了良好的效果。

参考文献:

[1] 谢喜秋, 梁洁, 等. 网络流量采集工具的分析和比较[J]. 电信科学, 2002, (4): 63-66.

[2] 岑贤道, 安常清. 网络管理协议及应用开发[M]. 北京: 清华大学出版社, 1998.

[3] 卢苇, 严斌宇, 等. MRTG 软件在校园网状态参数监测中的应用[J]. 四川大学学报(自然科学版), 2001, 38(2): 189-192.

[4] 丛锁, 吴甘沙, 等. 网络状态参数监测与 MRTG 的应用[J]. 微型电脑应用, 2000, 16(4): 51-55.

[5] MRTG: The Multi Router Traffic Grapher[EB/OL]. http://www.mrtg.org, 2004-09.

作者简介:

蒋海(1980-), 男, 硕士研究生, 研究方向为计算机网络与安全技术; 刘淑芬(1950-), 女, 教授, 博士生导师, 研究方向为计算机网络与安全技术。