文章编号: 1672 - 058X(2009)03 - 0282 - 04

基于开源软件的流量监控系统研究及实现

唐 勇
(重庆工商大学 网络管理中心,重庆 400067)

摘 要:阐述了流量监控在网络管理中的重要性以及网络流量监控的原理及方法,然后提出了以开源软件 Cacti搭建流量监控系统的方案,并介绍了该系统的主要功能及实现过程,最后给出了该系统的实际效果图及应用前景。

关键词:流量监控; SNMP; Cacti
中图分类号: TP393 **文献标识码**: A

随着教育信息化的深入,数字化校园建设的开展,高校网络支撑的业务越来越广泛,网络规模越来越大,结构日趋复杂,对网络的可靠性与可用性的依赖程度也越来越高,微小的网络流量变化都可能对网络关键应用造成重大的影响。因此,利用流量监控技术对网络运行状况进行全面分析,不但关系到网络的运行维护,而且成为网络管理中的一大挑战。

校园网经过长时间建设,网络设备型号多样,不同网络设备厂商提供的监测软件存在投入成本高,需要分别学习,管理困难等缺点。经过长时间摸索,可以采用软件监测的方法,利用 SNMP协议获取设备的参数与实时工作信息,并在浏览器上直观地显示出来。此处首先对 SNMP协议及流量监控原理进行了说明,介绍了基于此协议开发的开源网络流量监控软件 Cacti,然后详细介绍了 Cacti的安装配置及实现过程,同时给出了实际的监测效果。

1 网络流量监控原理及方法

在运行 TCP/IP协议的互联网环境中,管理协议的标准是简单网络管理协议 (Simple Network Management Protocol, SNMP),在该协议中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之间相互进行消息传送的规程。

1.1 SNMP基础

SNMP是一个应用层协议,是 TCP/IP协议族的一部分,通过用户数据报协议 (UDP)来操作,随着 TCP/IP成为事实上的协议标准而广泛被使用。SNMP主要由管理者、管理代理和管理信息库 (MIB)3部分组成,其中 MIB是对被管理设备中各个对象的性质和定义的集合,存放设备或者网络运行状态的信息。管理者可通过 SNMPGetRequest, GetNextRequest, SetRequest, GetResponse, Trap等操作获得和设置 MIB的参数值。

1.2 SNMP管理系统工作原理

管理进程通过定时向各个设备的设备代理进程发送查询请求消息 (以轮询方式)来跟踪各个设备的状

收稿日期: 2009 - 03 - 05;**修回日期**: 2009 - 04 - 10。

作者简介:唐勇 (1980 -),男,四川人,助理工程师,从事计算机网络建设及应用研究。

态;而当设备出现异常事件如设备冷启动等时,设备代理进程主动向管理进程发送陷阱消息,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,而被管理设备将其各种管理对象的信息都存放在 MIB库中。其中 SNMP协议运行在 UDP协议之上,它利用的是 UDP协议的 161/162端口。161端口被设备代理监听,等待接受管理者进程发送的管理信息查询请求消息;162端口由管理者进程监听等待设备代理进程发送的异常事件报告陷阱消息。

2　基于 SNMP协议的开源监测工具

MRTG是一套基于 SNMP的典型网络流量统计分析工具,它通过 SNMP协议从设备得到其流量信息并将流量负载以包含 JPEG格式图形的 HTML文档的方式显示给用户。MRTG的优点是简单易用,耗用系统资源小,但是其数据不能重复使用且无管理功能,其作者在多年前就已经开发了 RRDTool代替该软件,此外用来搭建流量监控系统的工具就是基于 RRDTool编写的 Cacti软件。

Cacti是一套基于 PHP、MySQL、SNMP及 RRDTool开发的网络流量监测图形分析工具。它通过 Snmpget来获取数据,使用 RRDtool绘画图形,而且完全不需要了解 RRDtool复杂的参数。它提供了非常强大的数据和用户管理功能,另外,它还提供了强大的数据管理和用户管理功能。在图像管理上,Cacti采用了树状结构的查看界面,在用户管理上,能对用户的权限进行细致划分,并且使用 LDAP进行用户验证。Cacti主要功能包括:可以指定每一个用户查看树状结构,host任何一张图,同时也能自己增加模板,功能强大完善,界面友好。

Cacti系统由 4个部分组成:Cacti页面 (PHP) —用户控制的平台,用户在此进行所有的设置;SNMP采集工具 —Unix下使用 Net-SNMP软件包自带的“snmpget”和“snmpwalk”等程序,Windows下使用 PHP的 SNMP功能;RRDTool绘图引擎 —性能数据的存储和绘画图像;MySQL数据库 —储存 RRDTool绘图所需的信息,如模板、rra、主机对应的信息等,要注意的是 MySQL数据库并不保存性能数据,性能数据保存在 RRDTool自己的数据库格式 rrd文件中。Cacti的工作流程如图 1。

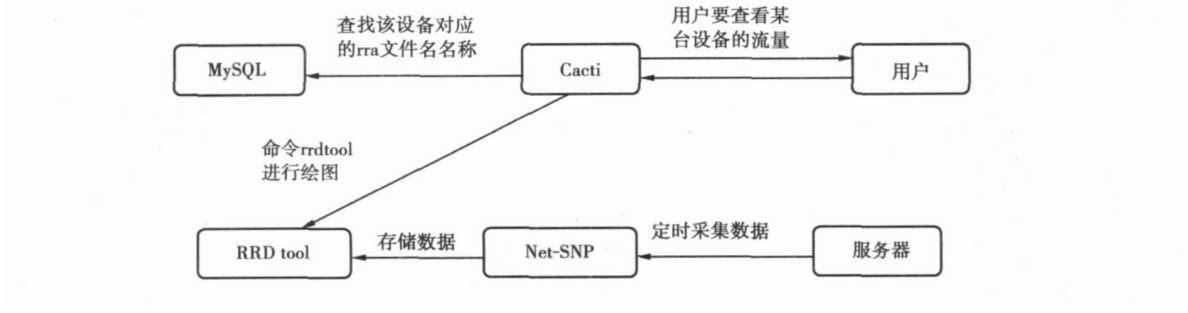

图 1　Cacti工作流程图

3　流量监控系统的实现

3.1　Cacti的安装及配置

用 Ubuntu作为流量监控系统的系统平台,Cacti基于 PHP、MySQL开发,依赖 LAMP环境,Ubuntu系统在安装时会提示选择是否安装 LAMP环境平台,只要选择安装即可。然后,利用 Ubuntu特有的 apt-get更新工具,直接从软件库中安装 Cacti以及所需软件,命令如下:MYM sudo apt-get install cacti,输入命令,系统会自动安装所关联的软件如 rrdtool、net-snmp等。重启 apache服务,在浏览器中输入相应的网址 http://cacti服务器 IP/cacti/访问,默认的用户名和密码都是 admin。具体的优化配置可以通过网络上广泛发布的文档来完

成,但针对 Cacti的网络流量气象图插件“weathermap”需要配制好。

3.2 Cacti应用及实例

以监控重庆工商大学出口路由器为例,路由器 IP地址为 10.20.20.1,开启 SNMP功能,修改 Community字符串 read值为“out1”,write值为“out2”,保存退出。在浏览器中访问 http://cacti服务器 IP/cacti/,输入用户名和密码进入 Cacti管理界面。单击“新建图像”,再点击“新建设备”,填写添加设备需要的信息,其中“设备模板”选择“udc/net SNMP设备”,“SNMP组”中将默认的“public”改为路由器的“out1”,单击“保存”保存信息。如果流量监控服务器及路由器 SNMP配置没问题,上方就会出现路由器的“设备名”“运行时间”等信息,否则会出现“SNMP错误”信息。

添加成功后,在下方的“相关数据查询”栏,添加数据查询,选择“SNMP-接口统计”,点击“添加”按钮,添加成功后就可看到该路由器所有端口的信息,选择要监控的端口即可。Cacti会自动创建监测点的 rrd文件、“数据源”条目和“图像管理”条目。

为了方便查看,可以将刚才新创建的设备图像加入到“图像树”上。单击“图像树”进入“图像树”面板,点击“添加”按钮添加新的“树项目”,在“树项目类型”选项中选择“设备”项目,“树项目值”选项的“设备”项目中选择刚才新添加的设备“路由器”,然后点击“创建”按钮。这样,就可以在“查看图像”界面中查看“路由器”的所有监测图像了。通过图 2,就可以看到校园网所有出口的流量监控数据。

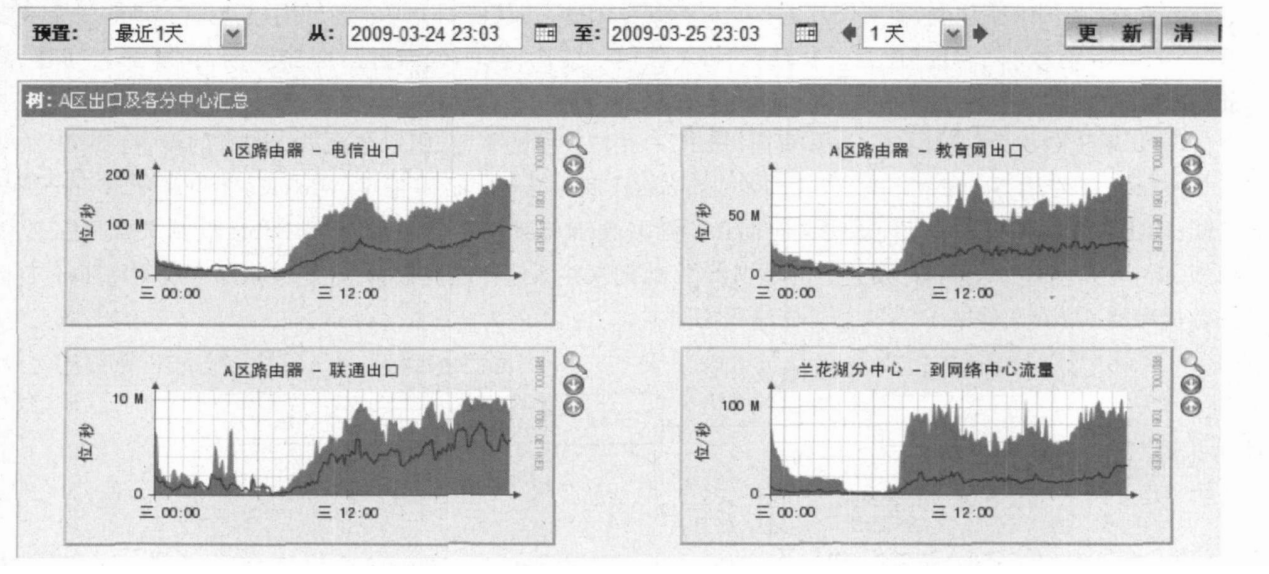

图 2 路由器流量监控图

最后,进入流量气象图配置工具,添加监控点和流量线路图,在流量线路中设定报警阀值,当各主干线路流量达到一定程度时,流量气象图会显示与占用带宽比例相对应的颜色。这样,在监控中心用浏览器将网页显示在大屏幕上,网络管理员即可实时查看校园网每隔 5 min采集的流量监测图。点击“weathermap”按钮,即可看到实际的网络流量监测气象图,如图 3。

通过图 3,可判断出校园网络在 21:00至 23:00是网络使用高峰期,而且这时的带宽非常吃紧,3个出口都是红色的报警线,带宽利用率都超过了 85%。这时,就必须根据自身情况增加出口带宽或者调整带宽来解决上网高峰期带宽资源不够的状况,以保证校园网的稳定运行。

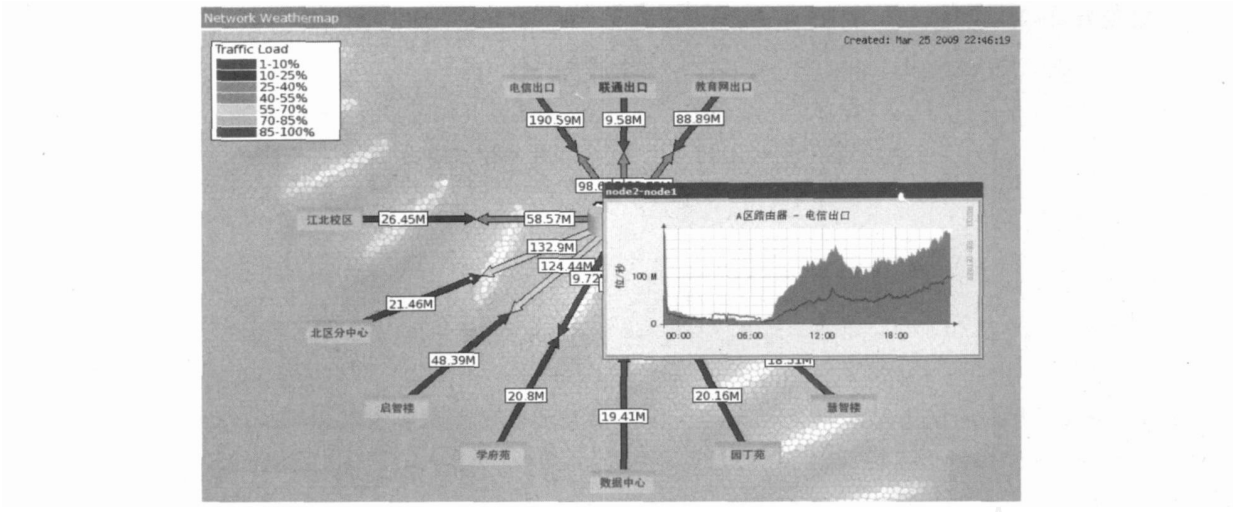

图 3　网络流量气象图

4　结束语

网络的流量监控在日常的网络运行维护中是一个重要的环节,利用 Cacti对网络设备进行流量监控和分析,可以直观地了解网络中各个部分的带宽使用情况,第一时间发现网络异常流量,有效防范黑客和病毒的攻击。同时,还可以根据各个端口使用带宽的情况对网络带宽进行合理划分,提高网络的运行效率。此外,Cacti是一款开源的软件,有许多如监控插件“monitor”、报警插件“threshold”等可以使用,还可以根据自身情况做二次开发。

利用这些插件,可以构建一个完全免费的网络管理系统,为学校节省大量的财力和物力,而且在以后的实践应用中可以逐步完善其功能。

参考文献:

[1]赵英,黄九梅,黄小国,等. 网络流量监控系统的设计与实现[J]. 计算机应用, 2004(6): 32-33

[2]秦国明. 异常流量分析和网络性能管理[J]. 中国金融电脑, 2005(3): 32-35

[3]唐政军,余芸珍,万利平,等. 基于 MRTG的校园网流量监控技术研究[J]. 南华大学学报, 2007(4): 92-96

[4]刘颖,刘景,郑海燕. Cacti在校园网络流量监测中的应用[J]. 电脑与电信, 2008(4): 10-14

[5]李向龙,刘晓龙. Cacti在校园网络流量监控中的应用[J]. 中国教育网络, 2007(12): 52-53

The research and implementation of flow monitor control system base on open-source soft

TANG Yong

(Network Management Center, Chongqing Technology and Business University, Chongqing 400067, China)

Abstract: This paper described the importance of flow monitoring in the network management and the principle and method of network flow monitoring, put forward the putting up of the flow monitor control system based on open-source software cacti, then introduced the main functions and implementation process of the system, and finally gives the effect drawing and application prospects of the system.

Key words: flow monitoring, SNMP, Cacti

责任编辑:李翠薇