

校园网络监测系统研究与设计

吕伟春, 胡洪新

(苏州市职业大学 发展与信息中心, 江苏 苏州 215104)

摘 要: 网络监测系统是基于 Cacti 的面向 RRDTOOL 的 B/S 系统, 在 MySQL 数据库中存储所有 RRDTOOL 创建图像所需要的信息及管理信息, 同时集成 Nagios 监控系统, 而所有的在监控范围内的主机信息及监控信息都存储在 MySQL 数据库中, 实现整个系统高度的整合. 采用软件工程中的原型法、并发开发法和试验法, 参照网络流量统计模型, 结合对开源软件的研究, 分析, 通过相关的程序设计、服务的配置以及设定相应的条件对主机和服务进行监控, 在状态变差和变好的时候给出告警信息.

关键词: 网络监控; 流量监控; 协议分析; Nagios

中图分类号: TH16; TP393

文献标识码: A

文章编号: 1000-7180(2010)06-0101-04

The Study and Design on the Campus Network Surveillance

LV Wei-chun, HU Hong-xin

(Center of Development and Information, Suzhou Vocational University, Suzhou 215104, China)

Abstract: The surveillance system is based on Cacti's B/S system towards RRDTOOL to store all the necessary information and management information RRDTOOL needs during the creation of the images and generate Nagios surveillance system, while all the host's information and the surveillance information in all the surveillance scopes to integrate the whole system. The paper adopts the prototyping, experimental method and concurrent development method in the software engineering, refers to the Internet flow model, combine the research and analysis of the open-source software, use the related programme design, the configuration of services and the set conditions to monitor the host and services to give the warning when the conditions are becoming bad or good so as to monitor the whole campus network.

Key words: network monitoring; flow control; protocol analysis; Nagios

1 引言

如今随着计算机网络技术的革新, 网络管理作为一项重要技术, 已成为数字化校园建设中不可或缺的一环. 同时由于网络规模不断扩大, 复杂程度不断增加, 异构性日益增强, 一个校园网络系统往往包含了若干子系统, 集成了多种网络操作系统、集合了不同厂商的网络应用设备, 同时还需要许多网络应用服务软件支撑. 因此, 我们需要一个高效的管理系统对网络进行有效的管理, 而网络监测是网络管理的重要内容.

早期各网络公司已经推出了很多商业化的网络

管理平台软件, 比如 SUN 公司的 SunNet Manager、HP 公司的 OpenView、IBM 的 NetView 等, 但这些平台对体现网络运行相关的历史数据的采集、管理、分析方面提供的功能都不能满足实际需要, 而且这些平台也存在某种不足: 管理成本高, 平台需要购买; 操作管理较烦琐, 必须由专业人士才能进行有效管理等诸多问题; 另外还需额外的网络带宽开销等. 因此, 文中介绍基于 Linux 的利用开源 (Open Source) 软件构建一个较为完善的网络监测管理系统, 以实现网络监测及故障的报警. 该平台在我校苏州市职业大学网络管理中起到了非常重要的作用.

基金项目: 苏州市职业大学科研基金资助项目 (SZD09L21)

收稿日期: 2009-07-12; **修回日期:** 2009-09-12

2 简单网络管理协议 SNMP

简单网络管理协议(Simple Network Management Protocol,SNMP)是由互联网工程任务组(Internet Engineering Task Force,IETF)定义的一套网络管理协议。

IETF 规定的管理信息库 MIB 中定义了可访问的网络设备及其属性,由对象识别符(Object Identifier,OID)唯一指定。MIB 是一个树形结构,SNMP 协议消息通过遍历 MIB 树形目录中的节点来访问网络中的设备。

举例:读取宿舍网核心设备 RG6806E 的 MIB 库,如图 1 所示。

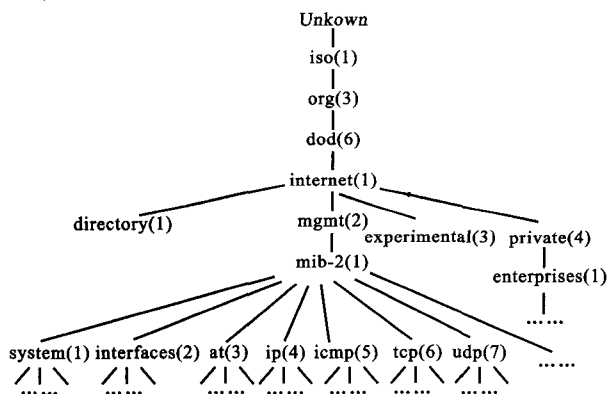


图 1 宿舍网核心设备 RG6806E 的 MIB 图

3 网络流量采集技术研究

网络流量分析^[1],是指通过一定的技术手段,实时监测用户网络 OSI 各层的流量分布,对网络协议、流量综合分析,从而有效地发现,预防网络流量和应用上的出现拥塞,为网络性能的稳定和优化提供依据。

端口镜像(Port mirroring),也叫做端口扫描或端口监控功能,是智能网管型交换机中的一个功能,其被用在一个网络交换机上来发送所有分组的拷贝,在一个交换机端口查看来监控在另一个交换机端口的网络连接。也就是把所有的交换机端口的数据,都拷贝一份到这个端口上,所有的数据都进行采集,该技术正是我校校园网络监测系统所采用的流量采集技术。

我校网络监测系统中对于数据流量监测的采集方法采用了基于 SNMP MIB 采集的方法。流量相关的主要采集参数是 MIB 库中的接口组部分:ifInOctets,接口发送的字节数;ifOutOctets,接口接收的字节数。

系统自 2009 年 3 月上线后不久发现,由于网络流量数据量较大,存在着 ifInOctets and ifOutOctets 统计溢出的情况,且对流量数据采集时出现了偏差。原因是由于 ifInOctets and ifOutOctets 的类型是 counter 是一个 32 位的无符号数,当流量超 100Mb/s 时,每 5 分钟采集一次流量就会出现溢出的问题。本系统中将 32 位的采集模型更改为 64 位的采集模型,SNMP 版本使用了 SNMPv2,此问题得以解决。

4 系统集成技术研究

系统集成是整个校园网络监测系统的一个关键,如何整合 Cacti、Ntop 和 Nagios 三大块是关系整个系统的运行和使用的价值,因此是整个系统设计的关键。

4.1 监控系统的运行及开发环境

整个监控系统分为三大块 Cacti、NTOP 和 Nagios,通过 Cacti 进行系统集成,是基于 Ubuntu 8.04.2 Server 平台的,使用 Perl,PHP 和 MySQL 数据库整合而成。通过对开源软件的再次开发,扩展达到网络监控的目的。

4.2 Cacti、Ntop 和 Nagios 系统集成框架设计

Ntop 和 Nagios 与 Cacti 整合是整个系统的关键,其架构如图 2 所示。Ntop 通过其插件实现与 Cacti 的整合^[2],达到管理员可直接调用 Ntop 系统,扩展了系统的目的。Nagios 与 Cacti 的整合同样系统采用了 Nagios 插件的形式完成,而其关键的整合技术是数据采集的入库问题,NPC 插件无法解决这个问题,而本系统使用了 NDoutils 来实现数据库的统一,实现了基于系统数据库的统一。

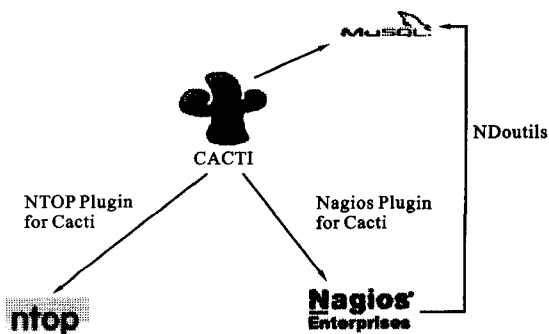


图 2 Cacti、Ntop 和 Nagios 系统集成框架图

4.3 Cacti 设计

针对我校网络的特点以及目前自身工作的关系,下面着重对校园宿舍网络中所涉及到的网络设备,特别是整个宿舍网络的核心、与教工网络互连设备、宿舍网络区域回聚和楼栋汇聚进行监测的配

置^[3].通过对各级设备的上下行流量、CPU 负载和内存利用率等信息的监测实现对整个宿舍网络设备的

的监控,如图 3 所示.

Description**	ID	Graphs	Data Sources	Status	Event Count	Hostname	Current (ms)	Average (ms)	Availability	
1#3760	9	3	3	Up	0	192.168.254.2	2.12	2.11	100	☐
10#3760	17	3	3	Up	0	192.168.254.38	2.69	2.11	100	☐
11#3750	7	11	11	Up	0	10.11.1.254	2.14	2.4	100	☐
12#3760	18	3	3	Up	0	192.168.254.46	2.73	2.11	100	☐
13#3760	19	3	3	Up	0	192.168.254.50	2.64	2.11	100	☐
14#3760	20	3	3	Up	0	192.168.254.54	2.73	2.11	100	☐
15#3760	21	3	3	Up	0	192.168.254.58	2.62	2.4	100	☐
16#3760	22	3	3	Up	0	192.168.254.62	2.45	2.11	100	☐
17#3760	23	3	3	Up	0	192.168.254.66	2.16	2.3	100	☐
18#3760	24	3	3	Up	0	192.168.254.70	2.16	2.75	100	☐
19#3760	25	3	3	Up	0	192.168.254.74	2.22	2.3	100	☐
2#3760	10	3	3	Up	0	192.168.254.6	2.07	2.11	100	☐
20#3760	8	3	3	Up	0	10.20.1.254	2.16	2.21	100	☐
21#3760	26	3	3	Up	0	192.168.254.82	2.16	2.3	100	☐
22#3760	27	3	3	Up	0	192.168.254.86	2.12	2.28	100	☐
3#3750	6	12	12	Up	0	10.3.1.254	2.15	2.39	99.98	☐
4#3760	11	3	3	Up	0	192.168.254.14	2.06	2.12	100	☐
5#3760	12	3	3	Up	0	192.168.254.18	2.16	2.12	100	☐
6#3760	13	3	3	Up	0	192.168.254.22	2.07	2.11	100	☐
6309	3	2	2	Up	0	192.168.100.254	2.02	2.11	96.87	☐
6806	4	4	4	Up	0	172.17.11.1	2.08	2.16	100	☐
6806a	2	4	5	Up	0	172.17.11.1	2.08	2.16	100	☐
7#3760	14	3	3	Up	0	192.168.254.26	2.54	2.12	100	☐
8#3760	15	3	3	Up	0	192.168.254.30	2.58	2.11	100	☐
9#3760	16	3	3	Up	0	192.168.254.34	2.67	2.12	100	☐
xiogong#3760	28	3	3	Up	0	192.168.254.90	2.08	2.07	100	☐
RC6806E	29	10	10	Up	0	192.168.254.253	2.18	2.1	100	☐

图 3 校宿舍网络核心设备监控图

4.4 Ntop 设计

Ntop 流量监测系统主要实现对数据流量的采集、分析及形成相应的报告,对异常流量查看,分析产生网络问题的原因,找到源头予以解决,从而保障整个网络的通畅^[4].

Ntop 系统在整个监测系统中是起到辅助作用的,但无法替代.它起到的功能就像当网络出现问题时我们使用 Sniffer 软件去检查网络流量和数据包是否异常一样.有了 Ntop 的辅助,我们可以随时随地地对当前网络中的数据包进行观察、分析,将网络故障的发生消灭于萌芽之中,因此对完善整个监控系统是非常重要的.

Ntop 系统由数据包捕获、数据包分析、后台数据库及前台显示等四个部分组成,如图 4 所示.

4.5 Nagios 设计

Nagios 设计主要围绕以下目标展开:

- (1) 被监控服务或设备状态信息的准确性;
- (2) 实现监控各种网络服务(Web,Mail 等);
- (3) 解决实际网络中存在的问题;
- (4) 有较强的灵活性;
- (5) 对各种集群设备进行监控;
- (6) 监控各类设备的硬件信息(内存与 CPU 占

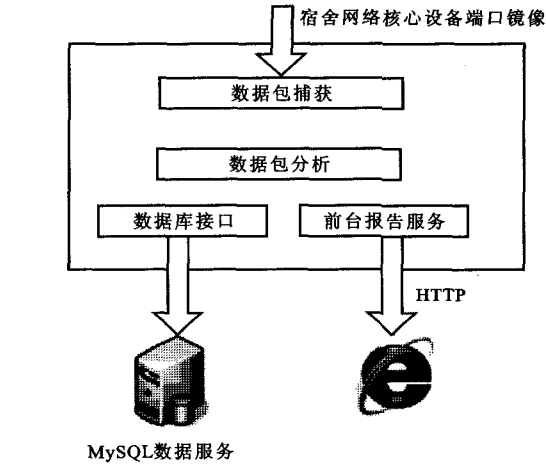


图 4 NTOP 系统架构

用率等);

- (7) 实现短信、Email 等方式的报警;
- (8) 简单易用性,容易维护.

Nagios 是整个设计中最关键的组成部分^[5],如图 5 所示. Nagios 能较好地实现与现有的系统框架结合. Nagios 通过内部与外部的插件实现与现有软件的集成,最终实现对被监控设备与服务的状态监控^[6].

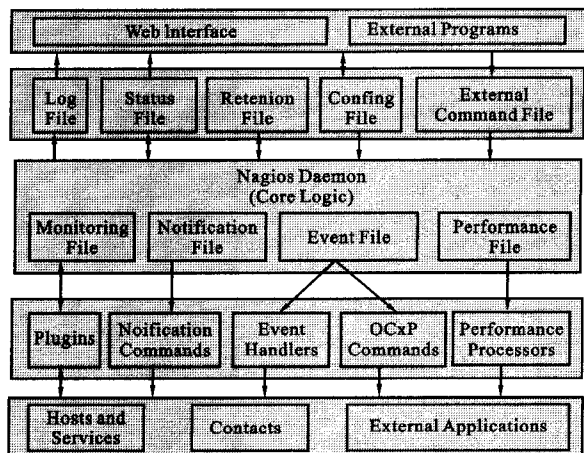


图 5 Nagios 系统框架

(资料来源: Nagios 在线帮助中文版 <http://nagios-cn.sourceforge.net/>)

5 结束语

系统将目前在 GNU 标准下的三大软件进行集成,大大降低了硬件成本与开发成本,很好地实现了校园宿舍网络部分的所涉及的服务器和网络设备的智能监控,还未推广至整个校园网络.校园网络监测监控系统主要由 Cacti, Ntop, Nagios 等监控和分析软件做系统集成,实现对宿舍网络计费服务器,自助服务器等设备的故障监控,对宿舍网络流量进行日常监控;实现故障、异常等信息以 email 等方式自动发送,及时通知系统管理员.

系统设计与实现中的经验与结论如下:

(1) 系统基于开源的思想,遵循 GNU 标准,提出了模块化设计方法实现校园网络监测系统的集成,体现了现代化大型软件的设计方法.

(2) 系统构建了以 Cacti 为中心, Nagios 为重要组成部分和 Ntop 为辅助工具的架构模型,在此基础上顺利完成了平台的搭建,系统已于 2009 年 3 月运行至今,未出现过任何异常.

(3) 系统实现了 Cacti, Ntop, Nagios 三者优势的融合,达到了对我校校园网络中所涉及到的应用服务器和网络设备进行监控的目的,简化了网络管理日常的工作,为我校网络中心提供了可靠的、完整的监控平台.

(4) 系统采用了数据库管理技术、有效灵活的报警机制,能够准确记录故障发生的时间和地点,为故障分析和及时解决提供可靠依据,同时提高了工作效率和解决问题的效率.

(5) 系统是基于开源软件做应用配置和集成,相对商业软件而言,开发和运行成本比较低廉,性价比较高,比较适合高校网络环境或中等规模网络环境.

参考文献:

- [1] 谢高岗, 闵应骅, 张大方, 等. 一个基于实际测试的网络流量模型[J]. 计算机工程与科学, 2001, 23(5): 51-53.
- [2] Dinangkur Kundu, Lavlu S M Ibrahim. Cacti. 0.8 network monitoring[M]. UK: Packt Publishing Ltd, 2009(8): 5-110.
- [3] 何斌斌, 周恩浩, 张波, 等. 基于 Cacti 的校园网络监控[J]. 科技信息, 2009(23): 60-61.
- [4] 赵冉. 网络流量测量系统 Ntop 的分析与研究[D]. 西安: 西北大学, 2008.
- [5] Dietmar Ruzicka. Network management with nagios, net-saint's successor, what's going on? [J]. Linux - magazine, 2003(4): 62-67.
- [6] Carla Schroder. Linux networking cookbook[M]. 冯亮, 译. 南京: 东南大学出版社, 2009: 426-487.

作者简介:

吕伟春 男, (1981-), 讲师, 硕士研究生. 研究方向为网络安全、网络技术、系统分析、系统集成等.

胡洪新 男, (1974-), 实验师. 研究方向为计算机应用研究.