

文章编号: 1674-5566(2010)02-0275-06

基于 web 的智能网管系统设计与实现

柯立新^{1,2}, 陈家琪¹, 吴开军²

(1. 上海理工大学光电信息与计算机工程学院, 上海 200093

2. 上海海洋大学现代信息与教育技术中心, 上海 201306)

摘要: 将简单网络管理协议 (SNMP) 的思想、NetFlow 技术、PHP 多线程技术融入到网络性能监测系统中, 通过对性能数据的采集、存储及分析, 设计并开发了一套智能化网管系统。系统采用 PHP 语言开发, 分为数据采集、性能数据库、数据分析及处理、数据显示、阈值设定与警告及用户管理 6 大模块, 不同的模块实现不同的功能。数据采集程序采用了多线程机制对性能数据进行采集, 多线程采集各种性能数据, 允许一个程序同时有效地执行多个任务, 既增强了程序的功能, 又提高了程序的性能。数据分析模块主要负责采集端口组、TCP/IP 组、UDP 组的数据, 并结合相关公式就可以计算出我们所需要的实时和历史数据性能指标值。信息显示模块按条件查询方式将端口组、IP 组、TCP 组、UDP 组的性能指标显示出来。实际应用证明, 该系统能够监控网络的实时变化, 并将异常及时地通过邮件、短信等方式反馈给网络管理员, 达到了预期目的。

关键词: SNMP; NetFlow; 智能网络管理; 多线程; PHP; OID

中图分类号: TP 393.06 **文献标识码:** A

Design and implementation of intelligent network management system based on web

KE Lixun², CHEN Jiaqi¹, WU Kaijun²

(1. School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China

2. Modern Information and Education Technology Center, Shanghai Ocean University, Shanghai 201306, China)

Abstract: SNMP protocol, NetFlow technology, multi-threading technology of PHP are introduced into performance monitoring system in this paper. A set of intelligent network monitoring system is designed and developed by collecting, storing and analyzing performance data. PHP language is used to develop the system. It is divided into six modules, such as data acquisition, performance databases, data analysis and processing, as well as data display, threshold settings and warnings and user management. Different modules achieve different functions. Data acquisition program uses multi-threading mechanism to collect a variety of performance data and allows the program to effectively perform multiple tasks simultaneously, so that it not only enhances the program's function but also improves the performance of the program. Data analysis module is mainly responsible for collecting data from the port group, TCP/IP group, UDP group and other groups, and combined with the relevant formulas, the real-time and historical data that we need can be calculated.

收稿日期: 2009-11-04

基金项目: 上海海洋大学青年基金 (A-2501-08-0127)

作者简介: 柯立新 (1980-), 男, 硕士研究生, 专业方向为网络安全。E-mail: kxl@shou.edu.cn

通讯作者: 陈家琪, Tel: 021-65684675, E-mail: cjq@126.com

Information display module displays performance of the port group, IP group, TCP group, UDP group and other groups according to the conditions search ways. Practical application shows that the system has achieved the expected goal by making overall performance more reasonable and improving the efficiency of operation of the campus network greatly through real time monitoring of performance data, and also reporting the exception to the network manager timely.

Key words: SNMP; NetFlow; intelligent network management; multi-threading; PHP; OD

随着计算机网络技术的迅猛发展,现代企业对于网络的依赖性越来越强烈。同时伴随着网络用户的不断增加和对企业级应用需求的不断提高,企业对于网络设备硬件的投入不断加大,于是各种各样的网络设备不断加入到企业局域网中,网络规模不断扩大,结构越来越复杂,功能也越来越强。网络管理已经成为网络系统运行好坏的关键。在网络发展的同时,人们更多关注网络设备的状态,关注网络中是否出现异常。设计一套高效的智能型网络性能监测管理系统尤为必要。其中网络管理协议是实现网络监测和管理功能必不可少的部分,简单网络管理协议(SNMP)由于其简单性,协议容易更新,并且可以方便地扩展功能以满足用户未来的管理需求,而被众多厂商支持。但是SNMP也有其自身的缺陷,它只能提供比较粗糙和简略的网络信息,这些信息只能让管理者发现部分问题,难以进一步对出现的问题采取相应的解决措施。为了克服上述存在的问题,本文在研究SNMP协议基础上,结合思科的NetFlow技术,设计并实现了一个针对企业网应用的网络性能监测管理原型系统。该系统采用了PHP语言进行编写,通过定时采集、监测和分析网络性能参数,使得网络整体性能更趋于合理,实现了对各种网元设备的统一管理,提高了网络运行的效率。

1 概述

1.1 简单网络管理协议(SNMP)

简单网络管理协议(SNMP)^[1-2]是TCP/IP协议簇的一个应用层协议,主要包括管理信息结构(MIB),管理信息库(MIB)以及SNMP协议。通过SNMP管理工具可以收集MIB信息,在管理控制台呈现给管理员这新信息报告设备的特性、数据吞吐量、通信超载和错误等,并能根据实际情况控制端口的通断等。

1.2 NetFlow技术

NetFlow技术是基于网流而发展起来的,是1996年由Cisco公司开发的一套网络流量统计技术。目前该技术已成为事实工业标准,被包括Juniper Extreme和Foundry等大多数主流网络设备提供商的支持^[3]。NetFlow技术利用流信息,可依据源IP地址、目的地IP地址对数据包进行包个数、字节数的统计。其根据网络数据包传输时连续相邻的数据包通常是往相同目的地地址传送的特性,配合Cache快取机制,利用标准路由模式处理数据流的第一个IP数据报,生成NetFlow缓存,随后同样的数据基于缓存信息在同一个数据流中进行传输,不再匹配相关的访问控制等策略,同时NetFlow缓存包含了随后数据流的统计信息。NetFlow目前主要有V1、V5、V7、V8、V9等5个版本。本文所使用的是NetFlow V5。

2 智能网管系统设计

本系统的目标是监测网元设备(路由器、交换机、主机)以获得网络性能参数,通过监测和分析网络性能参数^[4],不仅能直观地反映整个企业主干网络的动态变化和负载状况,而且还可以通过历史数据的统计和分析确定利用率趋势,预先发现网络运行瓶颈,并将异常及时的通过邮件、短信等方式反馈给网络管理员,从而避免网络饱和带来的低性能,更好的保障整个网络的顺畅。

2.1 系统总体架构

通过对网络管理、SNMP协议和NetFlow技术的研究,设计和构建了基于B/S架构的智能网络管理系统结构模型(如图1所示),分为数据采集、性能数据库、数据分析及处理、数据显示、阈值设定与警告及用户管理6大模块,不同的模块实现不同的功能。各模块结构如图1所示。

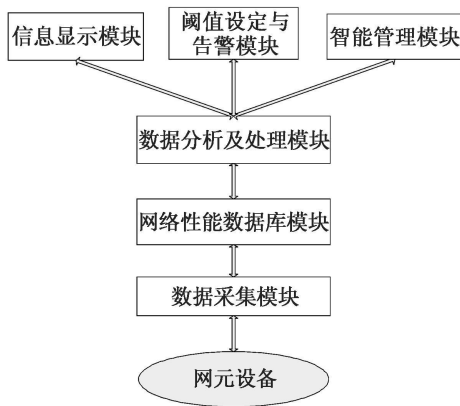


图 1 智能网管系统体系结构图
Fig 1 Intelligent network management system architecture

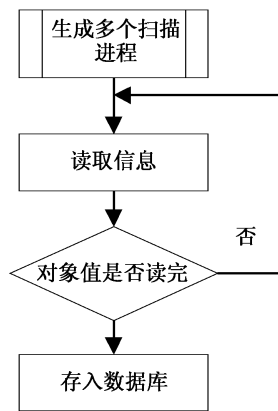


图 2 数据采集流程图
Fig 2 Data acquisition process

2.2 系统各模块功能

数据采集模块的功能是完成性能数据的实时采集, 并将采集的数据存入性能数据库, 其数据采集具体流程如图 2 所示。数据采集模块是性能监测系统的第一个环节, 是数据分析和显示的基础, 数据采集的准确性、实时性是影响企业网络的关键因素。为了加快采集的反应速度和更好的利用系统资源, 此数据采集程序采用了多线程机制对性能数据进行采集, 多线程采集各种性能数据, 允许一个程序同时有效地执行多个任务, 既增强了程序的功能, 又提高了程序的性能, 有了多线程的支持, 对数据采集就可以并发进行, 此程序每隔两分钟对数据进行一次采集、存储。性能数据库模块主要用于将数据采集到的性能数据存入相应的数据库中, 以供统计分析和显示模块等使用。因为网络流量大, 且变化较快对数据库的稳定性和速度要求较高, 另外考虑到跨平台, 因此本文选用 MySQL 数据库来存储原始流量信息^[5]。

数据分析模块主要用于采集端口组、TCP/IP 组和 UDP 组的数据, 并结合相关公式就可以计算出所需要的实时和历史数据性能指标值, 比如接口利用率、丢包率、错误率和转发率等。利用率反映了信道利用程度, 利用率高说明信道资源得以充分的利用, 而过高的利用率预示着信道可能成为潜在的网络瓶颈, 有必要进行升级。接口的输入输出丢包率反映了被丢弃报文所占总报文的百分比, 长期的高丢包率说明没有充分的处理报文^[9]。

信息显示模块包括实时显示子模块和历史数据显示子模块。实时显示子模块显示方式为利用即点即现方式和按条件查询方式将端口组、IP 组、TCP 组和 UDP 组的性能指标实时显示出来。即点即现方式就是将鼠标放到网络拓扑图的某条链路上就能动态显示该链路的多项性能指标; 按条件查询方式就是用户通过输入 IP 地址、端口号、选择指标 (例如端口利用率) 和图形 (折线图、点状图和柱状图) 就可以查询所有与性能相关的实时数据, 包括接口发送的字节数、接口接收到的字节数、接口利用率、输入/输出丢包率和 IP 吞吐率等。历史数据显示子模块显示方式为利用按历史条件查询方式将端口组、IP 组、TCP 组和 UDP 组的性能指标以折线图或饼形图的形式显示出来。按历史条件查询方式就是输入设备名称或 IP 地址, 选择时间、端口号及性能指标就可以查询过去任意与性能指标有关的性能图形。

阈值设定及告警模块是由于影响性能管理的性能指标很多, 如丢包率、交换机内存利用率和吞吐率等, 因此有必要对这些性能指标进行阈值设置以方便网络性能出现问题时可以及时向管理员告警^[7]。但是决定把阈值设置为多少是件很困难的事情, 一般情况下, 可以通过试验找到一个合理的数值^[8]。当设备的性能指标超过阈值时, 系统会发出告警并通过邮件或短信告知管理员。

智能管理模块是当网络出现异常, 系统会采用一些相应的策略来保证网络尽可能的正常运行^[9-10], 如尽可能保证比较重要的服务, 使损失

降低到最小。

3 实验结果及应用

3.1 系统运行环境

本系统以网络中心接入层和汇聚层交换机及一台服务器作为监测设备,编程语言采用 PHP语言,数据库采用 MySQL数据库,开发工具采用 Zend Studio 6.1.0。本系统采用标准的 SNMP协议结合 NetFlow,系统开发采用 PHP语言,网络监控模块采用了功能强大的 RRDTool,最后部署在 ubuntu9.04 server上。

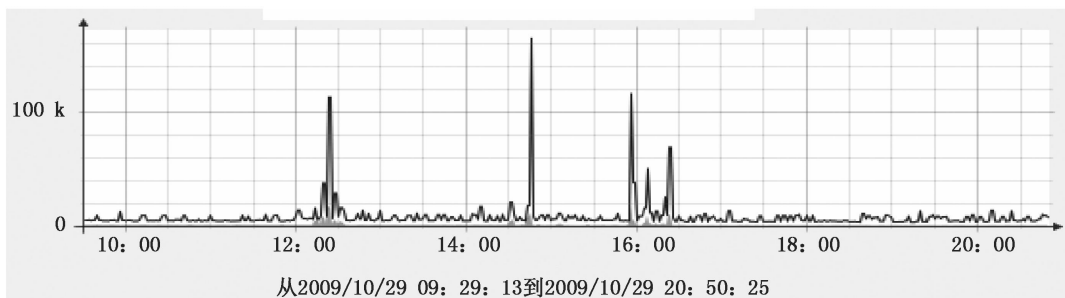


图 3 交换机端口流量曲线

Fig 3 Switch Port traffic curve

通过阈值与告警模块,能看到设备的状态(如图 4),及时发现网络问题,预防很多网络故障,当网络发生故障时,系统会自动发送电子邮件报告给网络管理员,实验中设置收件箱为 139 邮箱,邮件会以短信方式发到手机。



图 4 设备状态图

Fig 4 States of devices

4 结束语

本文设计并开发了一套基于 web 的智能网络管理系统,该系统采用 PHP语言编写,通用性好,可扩展性强,使用简捷、直观、方便,实验证明能实时监控网络设备和链路状态并智能处理一些简单网络故障。但是如何应用人工智能、神经网络相关理论来增强网络管理中的主动性、智能性,使网络可以自动及时地调整自身状态,减少

3.2 性能显示

系统的性能显示就是将采集到的性能数据以图形方式表现出来,PHP拥有强大的动态图形创建功能,这也是系统选用 PHP作为开发语言的重要原因之一。性能显示可以是实时的或历史的,通过校园网性能监测实时显示图(如图 3所示),可以看出链路流量、链路利用率情况以及整个主干网络拓扑的动态信息,以便网络管理员能更好的调控网络流量,使网络整体流量趋于合理,从而提高网络的整体性能。

人工参与,还有待我们进一步研究。

参考文献:

- [1] 马卫国. 计算机网络管理[M]. 北京:机械工业出版社, 2006
- [2] 杨家海,任宪坤. 网络管理原理与实现技术[M]. 北京:清华大学出版社, 2000
- [3] 李兴国,费玲玲. 基于 Netflow 的流量分析技术研究[J]. 微计算机信息, 2008 19(5): 198-200
- [4] 孙晋成,马力,殷春霞. 基于 SNMP 的校园网性能监测系统的设计与实现[J]. 西安邮电学院学报, 2009 14(3): 87-91
- [5] 张华忠,王勇. 多媒体网络实时监控平台的设计与实现[J]. 小型微型计算机系统, 2000 21(7): 770-772.
- [6] 翟有甜. Netflow 原理以及在互联网流量分析中的应用[D]. 上海:华东师范大学, 2006: 15-30
- [7] 张慧丽. 基于 Netflow 的异常流量智能检测引擎设计[J]. 计算机时代, 2006 (9): 17-19
- [8] 方匡钊,姚奇富. 基于统计预测算法的新型网络性能预警系统[J]. 计算机仿真, 2007 (8): 106-109
- [9] 汪精明,赵晓峰,王平水. 基于 Netflow 的蠕虫病毒监控系统设计与实现[J]. 计算机技术与发展, 2007 (5): 25-28.
- [10] 蒲天银,秦拯. 基于 Netflow 的流量异常检测技术研究[J]. 计算机与数字工程, 2009 (7): 115-118