SNMP 管理模型下的网络流量监视与控制

朱创录
(渭南师范学院 数学与信息科学学院,陕西 渭南 714000)

摘 要:随着网络规模的增大和网络结构的复杂化,计算机网络中的设备根据不同的应用需求,数量和种类也非常繁多,网络管理的难度也随之加大,其中一个重要问题就是对网络流量进行分析、统计以及控制。通过 SNMP 协议对 MIB 实时采集,可以实现网络流量监测,当网络核心节点端口出现流量异常的情况下,向防火墙发送控制指令,实现针对不同服务优先级别的网络应用进行流量控制,可以有效保障重要的网络应用需求在高峰时段的速率,并且可以实现在网络使用的空闲时段满足低优先级的网络应用。

关键词:SNMP;管理信息库;流量监视;流量控制
中图分类号:TP39 **文献标识码**:A **文章编号**:1673-629X(2013)08-0223-04
doi:10.3969/j.issn.1673-629X.2013.08.057

Monitoring and Control of Network Flow Based on SNMP

ZHU Chuang-lu
(College of Mathematics and Information Science, Weinan Normal University, Weinan 714000, China)

Abstract: With the increase of the network size and the complication of the network structure, according to various application demand for the equipment of computer network, the amount and type are very diverse, network management becomes more and more difficult. One of the key problems is analysis, statistics and control of network flow. Through SNMP finish real-time acquisition for MIB, monitor the network flow. When an exception occurs in the core node, management station sends the control instruction to firewall. According to the different priority of application, can realize control of the network flow to guarantee the rate for important network application demand during peak hours, and meet the network application with low-level in free time of network.

Key words: SNMP; MIB; flow monitor; flow control

0 引 言

对网络中的流量信息进行监测是实现网络管理及时发现网络出现的异常情况的重要手段,当前广泛使用的 SNMP 网络管理系统当中,采用读取代理上的 MIB-2 相关功能组中的管理信息并通过运算得到网络流量的信息,从而可以实现有效的管理监视,根据监视数据对网络的资源分布、性能评价、异常处理等进行相关操作。

网络流量监视的研究相对比较成熟,文献[1]中采用设备以及 OID 扫描的方法进行流量监测;文献[2]中根据网络流量历史值用灰色模型 GM(1,1)进行预测,并采用自适应过滤法对 GM(1,1)预测时产生的残差进行修正,从而达到较高的预测精度,进一步实现网络流量控制;文献[3,4]中采用网络协议分析的方法进行流量监测。以上研究大都把重点集中在网络流量监测方面,如何在网络流量监测数据的基础上实现流量的控制文献[5]中采用了 Linux 下的监控,基于 Linux 防火墙的网络数据包匹配过滤技术和 Linux 的流量控制技术进行流量控制。文中在参考文献[6,7]的基础上提出了采用阈值管理的方法结合不同网络应用的优先级别,动态实现网络流量的必要和非必要两种情况下的不同控制方法,采用 Windows Server 2003 环境下的 WinSNMP API 接口,使用 VC++6.0 作为开发环境,设计并实现了网络流量的监视与控制系统,该设计无需增加附加设备和改动网络的整体结构,在不增加网络管理负担的前提下,实现了基于 SNMP 协议的网络流量的监视与控制方案,广泛使用当前的网络管理环境,具有良好的可移植性和灵活性。

收稿日期:2012-11-16 **修回日期**:2013-02-20 **网络出版时间**:2013-04-22
基金项目:陕西省教育科研计划项目(12JK0746)
作者简介:朱创录(1977-),男,陕西兴平人,讲师,研究方向为网络应用和网络安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20130422.1721.022.html

1 SNMP 管理模型

SNMP 同它定义的管理信息库 MIB 共同提供了一种系统地监控和管理计算机网络的方法[8]。作为因特网的主要管理模型,SNMP 已经成为网络管理技术的事实标准。它管理局域网和广域网中的各种网络设备,包括路由器、UNIX 工作站和 PC 机。简单网络管理协议,使网络设备彼此之间可以交换管理信息,使网络管理员能够管理网络的性能,定位和解决网络故障,进行网络规划[9]。如图 1 所示,SNMP 管理模型具备典型的客户/服务器体系结构,其网络管理模型由四部分组成:

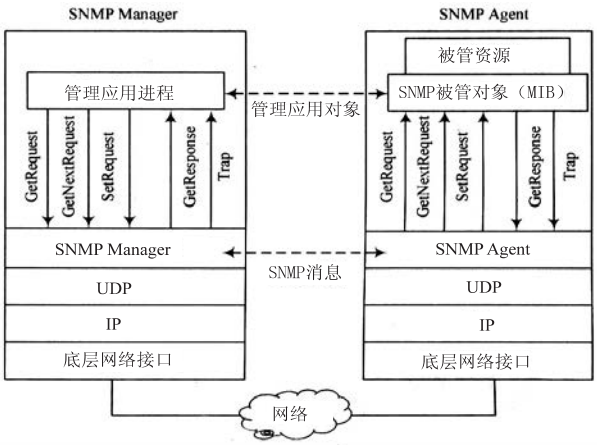

图 1 SNMP 的网络管理模型

a)管理站(Manager)是一个独立的设备或者是一个共享网络中的一员,为管理者和网络管理系统提供接口。

b)管理代理(Agent),一般厂家的网络产品如路由器、交换机等在出厂时都已配置好相关的 SNMP 管理代理,对于不支持 SNMP 协议的设备,可以开发委托代理(proxy agent)来支持 SNMP 协议。管理代理的功能是响应从网管站发出的读取请求(Get)和设置请求(Set),并且给网管站发送事件及告警信息(Trap)。

c)管理信息库(MIB)存放了该设备上被管对象资源的所有信息,每个被管对象有一个唯一对象的对象标识符(OID)。

d) SNMP 网络管理协议主要具有以下三个功能:①取值(Get)使网管站能够从代理处获取相关对象的值;②设置值(Set)使网管站能够在代理上设置相关对象的值;③告警信息(Trap)使代理能够通知管理站、代理端(Agent)的管理信息库 MIB 值的重大变化以及其他重要事件发出。

2 流量监测的 MIB 功能组以及控制方法

2.1 流量监测方法

影响网络响应速度的关键网络元素是核心交换节点,因此对核心交换节点的网络流量监测是分析网络流量异常的先决条件,要实现对网络进行流量的监测方法比较多,研究也相对成熟,这里采用 SNMP 协议实现对核心节点 MIB-2 库中能够反映网络流量的相关对象进行访问,达到有效监视管理的目的。MIB-2 库中能够反映网络流量的对象集中在 IP 组,TCP 组,Interface 组以及 ICMP 组,其中对 Interface 组中 iftable 表的访问可以获得核心交换节点的流量数据,为进一步实现流量控制提供判决依据[10]。流量监测的相关指标和 MIB 对象之间的计算方法如表 1 所示。

表 1 监测指标和 MIB 数据之间的运算

编号	监测指标	MIB 对象计算方法
1	进出流量总计	△ifInOctets+△ifOutOctets
2	端口带宽利用率	(△ifInOctets+△ifOutOctets)/(△ t * ifSpeed)
3	输入速度	△ifInOctets/△ t
4	输出速度	△ifOutOctets/△ t
5	输入错误率	△ifInErrors/(△ifInUcastPkts+△ifInNUcastPkts)
6	输出错误率	△ifOutErrors/(△ifOutUcastPkts+△ifOutNUcastPkts)
7	输入丢包率	△ifinDiscards/(△ifInUcastPkts+AifInNUcastPkts)
8	输出丢包率	△ifOutDiscards/(△ifOutUcastPkts+△ifOutNUcastPkts)
9	IP 数据报输入速率	△ipInReceives/△ t
10	IP 转发速率	△ipForwDatagrams/△ t
11	IP 丢弃率	△ipInDiscards/△ipInReceives
12	IP 无路由率	△ipOutNoRoutes/(△ipForwDatagrams+△ipOutRequests)

注:在不同的两个时刻,采集两组数据,Δt 表示时间差, ΔX 表示 X 对象值之差

流量监控主要用到公式(1)和公式(2),如下:

$$Flow_{in} = \Delta ifInOctets/\Delta t \quad (1)$$

$$Flow_{out} = \Delta ifOutOctets/\Delta t \quad (2)$$

公式 1 中的 ifInOctets 在 MIB-2 库中来自 interface 组,其 OID 值为 1.3.6.1.2.1.2.2.1.10;公式 2 中 ifOutOctets 在 MIB-2 库中来自 interface 组,其 OID 值为 1.3.6.1.2.1.2.2.1.16;时间 t 来自 system 组中 sysUpTime 对象,其 OID 值为 1.3.6.1.2.1.1.3。

从公式中可以看到,流量计算其实是 MIB 中统计标量的运算,所以要利用公式(1)和公式(2)计算流出流量和流入流量时,其中的关键问题是轮询周期的设置,如果轮询周期设置过大,则影响流量的实时性,不能准确反映某个具体时间点的流量情况,如果流量周期设计过小,则管理站会高频率的向核心节点交换设备发送 SNMP 协议的 Get 命令,导致代理设备为响应管理站的 Get 请求而花费大量的资源,从而影响代理节点的正常通信功能,因此在设计轮询周期时要根据具体的网络环境进行修正。

2.2 流量控制方法

表 1 中的接口速度以及宽口的带宽利用率反应了接口的利用情况,其数据是动态实时显示的,要判断流量的异常必须提供参考的依据,可以通过阈值设置的

方法判断网络核心交换节点的网络带宽的利用情况,从而提供控制依据,如果超过阈值上限给网络流量控制服务器(这里可以采用 Linux 防火墙)发送检测和控制命令,通过流量控制系统对流量进行控制,实现对优先级较低的流量应用进行网络阻隔,而在网络流量不高时可以允许优先级较低的网络应用占用带宽。实现网络流量控制功能主要依赖于对网络应用的识别和管理以及优先级别的设置,网络应用的识别与管理包括以下几个方面:网络流量的测量分析、网络应用的识别、网络应用的控制与管理。其中“网络流量的测量分析”在 SNMP 管理站上通过表 1 中对象的监测数据运算得到;“网络应用的识别”主要针对网络中日益增多的 P2P 业务吞噬网络带宽而采取的必要措施,通过识别 P2P 业务数据,在网络带宽利用率高于上限时主动采取措施阻断 P2P 业务数据;“网络应用的控制与管理”是根据网络应用识别的结果,采取控制 P2P 等低优先级业务数据的方法,并根据“网络流量的检测分析”的反馈数据采取进一步的处理措施。针对不同的应用,在设计防火墙进行流量过滤时,将不同的业务数据流分为若干等级,等级较高的为必须满足网络带宽要求的数据或者是一些实时性要求较高的应用,等级较低的为一些 P2P 数据、视频流数据等。通过数据业务的等级区分,根据核心交换节点带宽的利用情况,动态地实现流量的控制。

图 2 为网络流量监视与控制,图 3 为流量监控流程图。

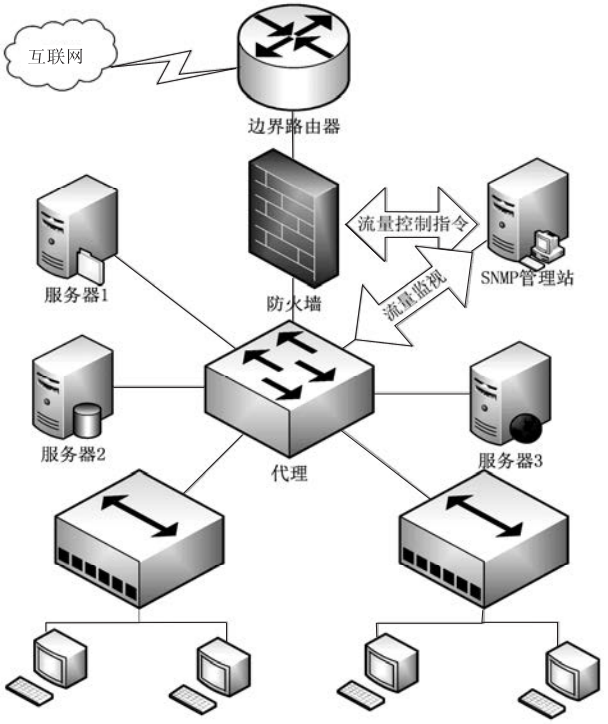

图 2　网络流量监视与控制

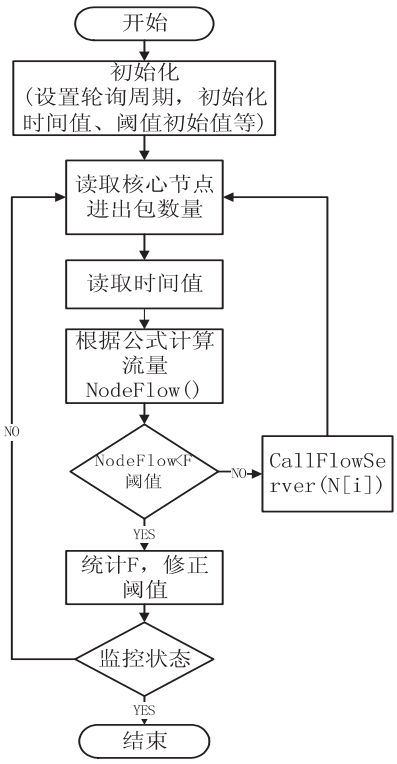

图 3　流量监控流程图

3　SNMP 网络流量监控功能实现

网络监控模型的实现是在 Windows Server 2003 环境下搭建 SNMP 管理站并运行流量控制实体的方式完成的,在 Windows 下实现 SNMP 协议的编程,可以采用 Winsock 接口,在 161,162 端口通过 UDP 协议传送信息,但在 Windows Server 2003 中,Microsoft 已经封装了 SNMP 协议的实现,提供了一套可供在 Windows 下开发基于 SNMP 的网络管理程序的接口 WinSNMP API,其目的是为在 Windows 下开发基于 SNMP 的网络管理程序提供解决方案,为 SNMP 网管开发者提供了必须遵循的开放式单一接口规范并且定义了过程调用、数据类型、数据结构和相关的语法,另外,WinSNMP 以函数的形式封装了 SNMP 协议的各部分并且针对 SNMP 在运输层使用 UDP 协议的特点设置了消息重传机制、超时机制等。

在实现过程中通过设置 OID 流量监测相关对象的取样周期,实时获取流量值,通过表 1 中的公式(1)和公式(2)进行运算,这里实现对网络出入口路由器和核心交换机实现流量监测,并且针对流量监测的结果进行阈值判断,当出现异常流量的时候,由 SNMP 管理站主动给流量控制服务发起控制指令,流量控制服务器根据应用的优先级以及协议使用情况终止 P2P 等优先级别低的网络应用。阈值的选择是高效实现流量控制的关键,选择时要充分考虑网络的使用周期,因为网络的使用情况和时间有很大的关系,所以这里不

能使用算术平均的方法,可以考虑采用与时间有关的加权平均值,也可以进行分时统计,这里采用后者。通过 FlowG [24]数组存放每一个小时的流量统计值,每个时间段的阈值采用略大于该时间段内平均流量的方法。

其实现过程主要包含三个部分:第一步,周期性发送查询相关 OID 命令;第二部,设置异步接收函数并处理接收到的数据;第三部,进行阈值判断,如果流量超过上限启动流动控制服务。以下列出了实现过程中三大部分的主要语句,采用 Visual C++环境下的 WinSNMP API 实现,其核心代码如下:

```
pSnmp.CreateVbl(OID,NULL);
for(int i=2;i<=6;i++)
{
pSnmp.SetVbl(m_initOid[i]);
}
pSnmp.CreatePdu(SNMP_PDU_GET,NULL,NULL,NULL);
pSnmp.Send(IPString,"public");
……
smiINT sNumber;
sNumber=m_value[i]->value.sNumber;
nIpin=sNumber;
wsprintf(str[i],"%d",sNumber);
NodeFlow=(ifIOOctetsL- ifIOOctetsH)/Dt;
……
if(NodeFlow>Fg)
CallFlowServer(N[i]);
……
```

4 结束语

针对当前共享带宽的园区网络中存在异常流量导致网络节点部分端口形成速度瓶颈,从而导致访问速度变慢的问题,利用 SNMP 良好的通用性和丰富的监控功能,结合异常流量的特点,构建了一种能够实时对网络重要节点端口速度进行监控的模型,其实现主要包括两部分,其一,通过 SNMP 协议访问监控节点的 MIB,实现对节点流量的监控;其二,对监控结果设置阈值,监控流量超过门限时进行流量的管控。该模型设计可以有效评价网络的运行状态,当出现流量异常时可以及时地采取措施,避免了传统的网络防火墙进行流量控制过程中数据分析量过大造成数据延迟的问题。该模型设计也存在不足之处:监控的网络规模不宜过大。在大规模网络下可以考虑采用分布式的网络管理模式结合控制模型的方法,这也是需要进一步研究的问题。

参考文献:

[1] 张 彤,吴世荣. 基于 SNMP 计算机网络流量监控系统研究[J]. 计算机技术与发展,2011,21(1):88-91.

[2] 马华林,李翠凤,张立燕. 基于灰色模型和自适应过滤的网络流量预测[J]. 计算机工程,2009,35(1):130-131.

[3] 吴烨虹,张少娴. 网络分析仪在网络流量监测中的应用[J]. 计算机技术与发展,2012,22(8):237-240.

[4] 严斌宇,刘方圆,吴少华. 基于 SNMP 的网络管理软件的设计与实现[J]. 计算机与数字工程,2012,40(4):126-129.

[5] 陆飞跃. 网络流量控制系统的分析及实现[D]. 北京:北京邮电大学,2010.

[6] Chang Yanan, Xiao Debao, Chen Limiao. Design and Implementation of NETCONF-Based Network Management System [C]//Proc. of 2008 Second International Conference on Future Generation Communication and Networking. [s. l.]:[s. n.],2008:256-259.

[7] 赵永胜. MRTG 在网络管理中的应用[J]. 铁路通信信号工程技术,2005(6):43-45.

[8] Choi M,Choi H,Hong J W. XML-based Configuration Management for IP Networks Devices[J]. IEEE Communications Magazine,2004,42(7):84-91.

[9] Schonwalder J,Pras A,Martin-Flatin J P. On the Future of Internet Management Technologies[J]. IEEE Communication Magazine,2003,41(10):90-97.

[10] 蔡 琳. 在 VC++6.0 平台下基于 SNMP 网络管理软件的开发[J]. 信息与电子工程,2005,3(3):224-227.

(上接第 222 页)

庆:重庆大学,2008.

[5] 李建林. 基于 Lucene 的 Web 搜索引擎的研究[D]. 兰州:兰州理工大学,2010.

[6] 邓 攀,刘功申. 一种高效的倒排索引存储结构[J]. 计算机工程与应用,2008,44(31):149-152.

[7] 李晓明, 闫宏飞, 王继民. 搜索引擎-原理、技术和系统[M]. 北京:科学出版社,2006.

[8] 李远方,邓世昆,闻玉彪,等. Hadoop-MapReduce 下的 PageRank 矩阵分块算法[J]. 计算机技术与发展,2011,21(8):6-9.

[9] Wu Hengliang,Zhang Weiwei. An Improved Page Ranking Algorithm for Web Search Engine[J]. International Journal of Digital Content Technology and Its Applications, 2012, 13(6):38-44.

[10] 刘青伟. 搜索引擎中的 Pagerank 排序算法研究分析[D]. 成都:电子科技大学,2010.

[11] Han Min,Zhang Xianchao. Community Identification Based on a New Approximate Personalized PageRank Algorithm[J]. Advances in Information Sciences and Service Sciences,2012,20(4):649-657.

[12] 李广丽,刘觉夫. 垂直搜索引擎系统的研究与实现[J]. 情报杂志,2009,28(10):144-147.

SNMP管理模型下的网络流量监视与控制

作者： 朱创录， ZHU Chuang-lu
作者单位： 渭南师范学院 数学与信息科学学院,陕西 渭南,714000
刊名： 计算机技术与发展
ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2013(8)