网络服务监视代理的设计与实现

邵文简
（东南大学计算机科学与工程系，南京 210096）

【摘要】对网络服务情况的监视和管理是网络管理中重要的一环。本文介绍一个网络服务监视代理的设计思想和实现方法，并对其中的数据采集策略、分析处理方法、结果调用接口等核心环节进行了分析和讨论。

【关键字】网络管理　服务　代理　SNMP　TCPDUMP

1．概述

目前 Internet 正在以前所未有的速度发展，随着 Internet 用户的成倍增加，网络流量也随之迅速增长。网络流量由多种网络服务组成，且组成情况十分复杂。在网络运行管理中要求能够对网络流量的组成情况，即网络提供的各种服务的分布状况进行监视。通过对网络服务的监视，我们希望实现一些更加高级的管理功能，例如：

- 提高服务质量(QoS)
- 对传输内容加以控制
- 优化带宽分配
- 平衡网络流量
- 快速发现网络故障原因

为了实现以上管理功能，首先要求能够得到 TCP 层和应用层报文信息的网络流量数据，按照管理要求对其进行网络服务的具体分析和统计，这就提出了新的挑战。因为目前从路由器的 MIB 中只能采集得到 IP 层的流量数据，而无法获得更加详细的 TCP 层以上的数据。因此我们设计并实现了一种网络服务监视代理，以实现对网络服务情况的监视。

本文论述了一种网络服务监视代理的设计思想和具体的实现方法。通过该监视代理对流进和流出的网络流量进行分析和统计，我们可以得到以下三个功能：

- 实时反映当前网络中的服务情况，包括网络的 IP 层、TCP 层和应用层的协议分布；报文长度分布；根据流量和报文数统计出当前各种服务的 TOP N 主机和 TOP N 链接等等。
- 以小时为单位，定时给出一小时内各个时段中，以上各项数据的统计结果。
- 对特定的链接进行实时或静态跟踪和分析。

2．设计思想

2．1 数据来源

有许多工具可以用来侦听以太网上的报文，如 Sniffer，Tcpdump 等。 Tcpdump 是美国加州大学伯克利实验室编写的一个基于 UNIX 操作系统的工具，它可以侦听以太网上的广播，从而得到同一个广播网段上所有主机传输的报文。采集得到的数据包括有 TCP 层和应用层的报头信息，只要将截取长度设置的足够大，还能够得到报文中实际的传输内容，有了这样详细的数据，我们就可以实现所要求的网络监控功能。虽然以太网侦听工具大都只能侦听处于同一个以太广播网段上的报文，但是只要适当地选择数据的采集点，我们还是可以用其采集数据。因此我们采用 Tcpdump 来完成网络的数据采集任务。

2．2 网络服务监视代理的模型

如图 1 所示，整个华东北地区网的各个子网都是接在地区网边界路由器 RGW 上，然后 RGW 通过一个以太网和主干网边界路由器 BGW 相连，再通过 BGW 接入 Cernet 主干网。我们用一台主机作为网络服务监视代理运行的设备，这台设备上配置有两个网络接口。其中的接口 1 处于连接 RGW 和 BGW 的以太网段中，这个接口用来侦听和采集所在以太网段广播的报文；接口 2 处于网络管理服务器所在的网段中，提供代理与外界进行通信的通道。使用了两个网络接口，监视代理就可以跨网段工作,代理的通信接口与被监视的网络分离增加了代理在使用中的灵活性。

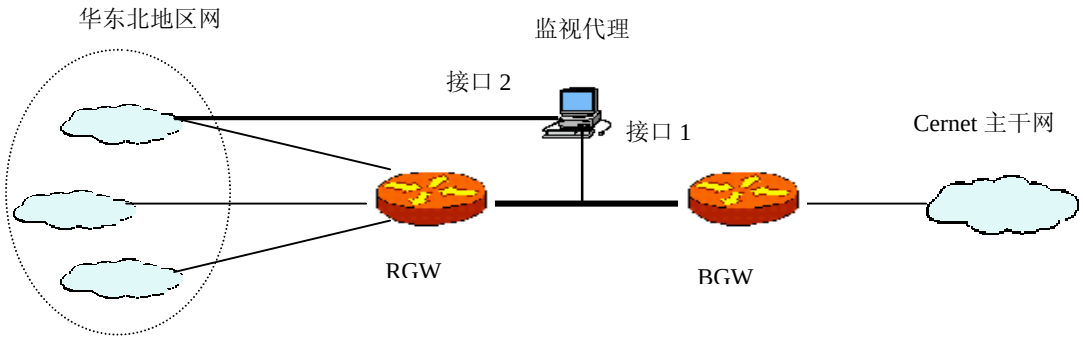

图 1 网络服务监视代理系统模型

如图 1 模型所示，接口 1 起到了一个探测器的作用，它可以采集所有流入和流出华东北地区网的报文，同时又屏蔽了网内各个子网间的流量，这就精简了数据，所以这是一个非常理想的数据采集点。通过应用不同的过滤规则，对采集得到的数据进行相应的分析和统计，我们就可以清楚的了解和掌握整个华东北地区网的网络服务情况。

这个模型虽然是针对华东北地区网的，但是对于大部分的校园网和企业网也是适用的，

可以作为网络管理系统中的有机组成部分。

2．3 数据预处理

采集得到的数据虽然屏蔽了子网间的流量，但是其数据量仍然很大，不可能长时间保存，必须及时地对采集得到的数据进行分析和统计，将大量的数据压缩为相关的结果。将这部分工作放在监视代理上完成既可以充分利用监视代理的运算能力，又可以减少网络传输负担。根据功能定义，监视代理实现如下的数据处理功能：

- 定时地对前一个小时的采集数据进行分析和统计，反映一个小时内的网络服务总体情况。根据报文的区域和流向特征，统计国内流入华东北地区；华东北地区流向国内；国外流入华东北地区；华东北地区流向国外的网络服务分布、报文长度分布情况和 TOP N 链接。并统计出华东北地区，国内和国外的各种服务的 TOP N 主机情况。根据用户的配置，将一个小时划分成若干个时段，对每个时段给出一个该时段内网络服务情况的报表，处理结束后就将采集的原始数据删除。定时处理产生的报表每个小时都更新一次，所以要将每次的报表存入网管数据库中，为进一步的分析提供数据。
- 实时地对当前若干长一段时间内的采集数据进行分析处理，反映网络当前的具体情况。时间的长度可由用户设置。生成的报表和定时的内容基本相同，报表是不断地更新，用户取得的始终是当前的网络服务情况报表。
- 根据用户提交的任务，对特定的链接进行跟踪和分析。将符合要求的报文存放在文件中供用户调用。

2．4 调用接口

分析和统计后生成的结果是关于网络服务情况的多种报表。将这些报表的各个表项和监视代理的工作参数都定义为相应的 MIB 变量，这样网络服务监视代理就成为了一个网络管理系统中标准的被管对象。可以通过简单网络管理协议 (SNMP)的 get 方法来访问监视代理生成的分析统计结果，通过 set 方法来对监视代理的参数进行配置，如定时处理的时间长度等等。用户提交链接跟踪任务也是通过 set 方法来实现的。

3．网络服务监视代理的实现

3．1 相关设备的配置

一般情况下，图 1 所示的两个路由器间的以太网段就是一根直接连接网线。所以需要用一个集线器来代替简单的网线来连接两台路由器和网络访问监视代理。

由于工作站及其附件都比较昂贵，而 PC 机的价格是相对便宜的，所以采用在 PC 机安装 Linux 操作系统环境来实现这个监视代理。在 PC 机上安装两块以太网卡来实现两个网络接口。

3．2 系统的实现

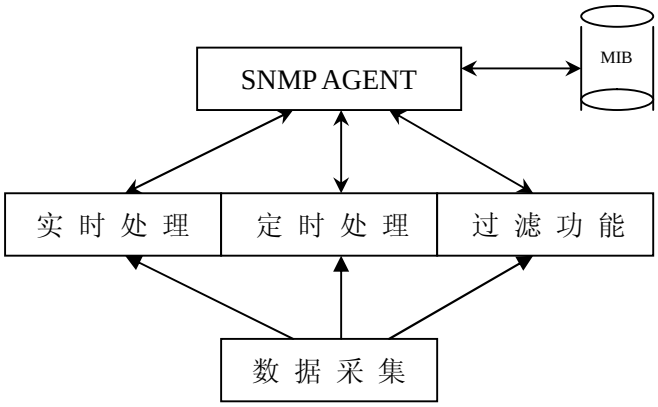

图 2 网络服务代理的模块图

图 2 是本网络服务监视代理的功能模块图。如图所示，本代理主要由三个部分组成：数据采集、数据处理和 SNMP AGENT。

数据采集部分的功能是利用 Tcpdump 来采集数据，它为上层的数据处理部分中的三个功能模块提供原始数据。数据采集模块采用双缓冲区的方法，用两个文件来轮换存储采集到的网络报文数据，一个存储当前这个小时内的数据而另一个用来存储前一个小时的数据。定时处理模块对上一个小时的数据文件进行分析和处理，而实时处理模块和过滤功能模块则对当前的数据文件进行处理。

数据处理部分由三个功能模块组成：

- 定时处理模块，以小时为单位来的统计网络服务情况。该模块进行报文读取，报头分析后得到报文的 IP 地址，TCP 和 UDP 端口号，报文长度等报文协议信息。通过对得到的信息进行分类，统计和排序等工作后生成需要的报表。
- 实时处理模块，实时地监视网络服务情况，该模块的处理过程和定时处理模块相似。为保证实时处理的实时性，实时处理进程要知道数据文件中指向当前最新一条报文的文件指针位置。指向当前文件末尾的指针不一定就是一条报文的起始位置，而可

能是一条报文的任何位置，因为每条报文的长度是不相当的，所以通过文件长度也无法推导出这个指针位置。为了解决这个问题，我们在采集模块中用一个子进程来跟踪最新报文的文件指针位置。为了实时处理进程能够访问这个变量，使用了共享存储区来存储该变量，该变量每秒钟刷新一次，可以保证实时处理进程的实时性。

- 过滤功能模块根据用户的要求将指定的服务和链接过滤出来，供用户分析；用户指定特定的 IP 地址和端口号，过滤功能模块从数据文件中将符合要求模块报文过滤出来，另外存放在一个结果文件中，供用户进一步分析。

SNMP AGENT 负责管理和维护管理信息库 (MIB)，负责通过 SNMP 协议和外部进行数据交互。

图中的三个部分共五个功能模块，每个功能模块都是一个独立运行的程序。由于每个功能模块是相互独立的程序，所以需要进程间的相互通信。数据处理部分的三个处理功能模块的结果都是以文件的形式存放，由 SNMP AGENT 将其以 MIB 变量的形式供外界访问，所以在这些处理进程和 SNMP AGENT 进程要使用文件锁来进行同步，防止读写进程同时对文件操作。而数据采集进程和实时处理进程间的通信要复杂一些，因为使用了共享存储区，所以在实时处理进程访问变量时和采集模块刷新变量时使用信号灯来实现同步。

3．3 进一步的工作

该监视代理虽然生成了许多网络服务的分析统计报表，但是为了详细和准确地反映网络服务的情况，还有许多需要加以完善的地方。通过对现有数据的进一步的分析，还可以更加完备的结果。例如，目前是根据各种网络服务的默认端口，即周知口(well known port)对网络服务进行分类的，对其他的端口没有做分析。通过对这部分端口进行分析，可以得到更详细的网络服务情况。

4．结论

通过对网络服务监视代理对网络服务的监视情况的统计分析，我们发现在网络正常运行情况下， WWW、 Ftp、Email 这三种网络服务类型占据了 Cernet 华东北地区网网络流量的 90%以上。对每一种服务类型而言，它们又有各自特征，如 WWW 服务呈现出明显的时间性，即在早八点至晚十点流量明显大于夜间休息时间，而 Ftp 和 Email 服务则变化趋势比较平缓等等。我们也发现各种服务流量在的各种应用服务总流量中所占的百分比也是有它们一定的规律的，这说明了当前主要网络应用服务的发展已相对稳定、成熟。

但是在网络发生故障时，网络服务情况就会出现异常的现象。如一个重要的子网如果出

现不通的故障，则会出现大量的发往该子网的 DNS 报文，导致整个网络服务质量下降。通过监视代理就会发现这时 DNS 服务所占的比例异常的大，这就有助于我们迅速的找出网络故障原因。

该网络访问监视代理的实现，不但能够及时准确地反映当前网络服务情况，而且能够体现网络服务情况的变化趋势，为网络管理提供了重要的数据。

参考文献

【1】Remote Monitoring Solutions for Wide-Area Networks: A Comprehensive WAN Monitoring Strategy for Enterprise Networks . Cisco Systems, Inc 1998

【2】NetScout Manager and NetScout Manager Plus for LANs, WANs, and Switched LANs. NetScout Systems, Inc 1997

【3】SNMP, SNMPv2, and RMON Practical Network Management. William Stallings

Design and Implementation of Network Services Monitoring Agent

【Abstract】Network Services Monitoring and Management is an important part of Network Management. This paper presents a way to design and implement such a kind of agent. The major issues about it, including the data collecting strategy, system analyzsing and dealing principles and the result interface solutions, are discussed in detail.

【Keywords】Network Management Services Agent SNMP TCPDUMP