基于 Netflow 的网络服务监测系统

吴 桦　　龚 俭　　张晓宇
(东南大学计算机科学与工程学院，南京 210096)
(江苏省计算机网络技术重点实验室，南京 210096)

摘要: 为了能通过 Netflow 得到网络性能测度，首先分析了从 Netflow 的长流信息中得到的网络性能测度的可信度, 然后设计了基于 Netflow 的网络服务监测系统, 该系统从历史数据中提取服务器的服务指纹作为服务质量的基准点，对用户关注的服务水平给出评判，包括数据分析方法、单个区域的变化规律和单个服务的服务指纹，并能根据网络状态的异常发现异常服务状况. 该系统对网络中新出现的应用具有可扩展性，有较好的应用前景.

关键词: Netflow; 服务; 服务质量; 服务指纹
中图分类号: TP393　　**文献标识码**: A　　**文章编号**: 1001-0505(2008)增刊(I)-0114-04

Netflow based network service QoS monitor system

Wu Hua　　Gong Jian　　Zhang Xiaoyu
(School of Computer Science and Engineering, Southeast University, Nanjing 210096, China)
(Key Laboratory of Computer Network Technology of Jiangsu Province, Nanjing 210096, China)

Abstract: In order to obtain the network performance metrics from the Netflow, the reliability of obtaining the network metrics from the sampled Netflow is analyzed. A Netflow based network service QoS(quality of service) monitor system is designed. The dactylogram of services can be distilled and used as the QoS baseline to judge the status of the services. The data analysis method, the variety of single zone's behavior and the dactylograms of services are described. The abnormity services can be detected by the exceptional status of the network. The system can be extended to new applications and have a good application prospect.
Key words: Netflow; service; QoS(quality of service); service dactylogram

网络应用的服务质量测度受到很多因素的影响，使用最小的代价得到用户的感知服务质量是一个难题. IETF 的 IPPM[1]工作组开发的测度标准测量代价较高，测量性价比较低. 测量的最终目的是维护网络正常服务，并非得到的结果越准确越好，而是用尽可能小的代价得到用户的服务质量感受.

流测量既可以满足细粒度网络管理的需求，在数据存储和处理开销上也具有较好的优势，在网络管理领域有很好的应用前景. Cisco 公司基于其硬件路由器产品的 NetFlow[2], 由于其标准的开放性而被业界厂商广泛支持. 这是网络管理者获得网络流信息代价最小的方法. 基于 Netflow 的网络管理系统可以对网络流量进行监测. 但是由于硬件资源的限制，Netflow 的流数据是经过采样后的报文数据组成的流记录，将 Netflow 应用到网络管理中必须考虑到抽样误差带来的影响. 尽管如此，由于 Netflow 流格式已经成为事实上的工业标准，基于 Netflow 数据的网络行为挖掘是当前的研究热点.

本文设计了一个基于 Netflow 流记录的服务监测系统，称为 SN-QoS（Sampled Netflow QoS）. 目前基于 Netflow 记录的网络管理基本是网络流量监测（计费，网络应用观测）和安全监测，本文将 Netflow 数据应用于服务质量估计，节约了以往使用主动测量得到性能的运行成本.

1 从 Netflow 长流中得到可信的服务质量测度

网络应用的服务质量可以从链路拥塞状况，往返时间，丢包率，抖动几个方面衡量，这几个方面是互相牵制的，不同的应用类型侧重点会不同. 最常用的是往返时间. ICMP 的 PING 是用来诊断网络状况的

收稿日期：2008-06-16. **基金项目**：国家重点基础研究发展计划（973 计划）资助项目(2003CB314804).
作者简介: 吴桦（1973－）,女,博士生,讲师; 龚俭（联系人）,男,博士,教授,博士生导师,jgong@njnet.edu.cn.

最基本工具 PING 是一种主动测试手段，需要主动发起测试报文，此外这个 RTT 是 ICMP 协议的，并非应用层协议，是通过发送很小的 ICMP 报文测得的，已有研究表明[3]，流速和流长具有相关性，因此使用 PING 得到的 RTT 和用户具体感受到的延迟还是有一定差距. 本文用流速表达得到的数据传输速度，流速定义为某个应用流在单位时间内传输给用户的字节数（或者报文数），以及在单位时间内接收到的用户字节数（或者报文数）. 由于流的双向传输不是完全对称的，为了简单起见，以下定义的流速为单向流.

定义 1　设流速为 v_{f},流的字节数为 O_{f},流的持续时间为 t_{f}，则流速定义为

$$v_{\mathrm{f}} = o_{\mathrm{f}} / t_{\mathrm{f}} \tag{1}$$

定义中的 2 个变量 O_{f}，t_{f} 都是需要从 Sampled Netflow 记录中估计出. 因此 v_{f} 的误差取决于 O_{f} 和 t_{f} 这 2 个量的估计误差，下面分别讨论这两个量对 v_{f} 估计误差的影响.

首先考虑 v_{f} 的估计误差和 O_{f} 的关系. 设 $\hat{o}$ 是对报文进行系统抽样后得到的单个流的字节总数，N 为抽样比，则 $\hat{O} = N\hat{o}$ 是原始报文总数 O 的无偏估计，即 $E(\hat{O}) = O$，且标准差为[4]

$$\frac{\sqrt{\mathrm{Var}(\hat{O})}}{O} = \frac{\sqrt{(N-1)\sum_{i=1}^{P} o_i^2}}{O} = \frac{\sqrt{(N-1)\sum_{i=1}^{p} o_i^2}}{N\hat{o}}$$

这个标准差公式说明流的原始字节总数 O 的估计的均方差随 N 增大而减小，大致上正比于 $\frac{1}{\sqrt{N}}$. 假设流的持续时间误差很小，流速的误差正比于流的原始字节总数估计的均方差，所以流速的误差随 N 增大而减小，在 $\hat{o}$ 相同的情况下，N 越大意味着流越长，那么在 N 固定的情况下，长流的流速估计误差较小. 另一方面，考虑流速估计值的误差与流的持续时间的关系. 为了定性地说明问题，假设长流的持续时间是相对稳定的（对一个特定流来说），当作常数看待，则可以对流速公式两边取方差，设流速和字节数的方差分别为 $s_{\mathrm{vf}}^2, S_{\mathrm{of}}^2$，即 $s_{\mathrm{vf}}^2 = \frac{s_{\mathrm{of}}^2}{t_{\mathrm{f}}}$，两边开根号得均方差：$|s_{\mathrm{vf}}| = \frac{|s_{\mathrm{of}}|}{t_{\mathrm{f}}}$. 由此可见，持续时间愈长的长流，其流速估计误差愈小；被抽到的报文越多的流，流速估计误差也愈小. 根据这个准则，在使用 Netflow 记录进行流速估计的时候，选择持续时间长，被抽中报文数目多的流记录作为服务质量计算的数据来源. 由于网络中流长的重尾分布特征[5-6]，只需要监测少量的长流就可以得到网络服务质量的估计，大大减少了分析的工作量和数据的存储量.

2　基于 Netflow 的服务器监测系统的流程设计

流速反映了单个流的服务质量测度，但是在网络服务中，单个流的流速不能说明应用的服务质量. 由于单个流的流速和用户个人的上网设备配置，应用类型以至生活作息习惯有很大关系，很难得到具有统计意义的基准值. 因此对网络服务质量的监控应该考虑具有较稳定特征的服务测度. 本系统对服务器上的流速进行统计分析，将当前的统计值和历史的统计值进行比较分析，以得到服务质量判断. 服务质量的评判不能完全脱离其应用类型，应用服务类型很多，并不断增加，应用的识别一直是研究的热点和难点. 本系统的设计必须能够避免服务识别，可以自适应地感知新的服务所具有的统计特性，以提高系统的可用性. 图 1 为网络服务质量监测系统的流程图.

这个系统的处理工作分为 2 个层次，第一层次是日常监控，将数据从路由器采集后，进行网络状态监测和服务器状态监测；第二层次是异常服务发现以及异常服务追踪. 通过这 2 个层次的监控，可以对用户访问量大、最广的服务资源的服务质量进行监控.

第一层的日常监控中，包含了网络状态监控和服务器监控 2 个模块. 其中网络状态监测是和基于 Netflow 的网络管理系统相关联的，对网络运行的日常状态进行监控，通过历史数据提供网络正常状态的基准值. 这个基准值并非指一个值，而是某个重要测度的变化趋势规律，通常可以通过对用户群观察建基准值，并建立预测模型，当得到的网络状态值和预测值偏差较大的时候，就认为出现了异常，进入第二个层次. 第一层除了网络状态监测外，还包含服务状态监测，如新浪，谷歌，这些服务器对用户所能提供

的服务会被用户视为对网络服务质量具有象征意义．此外这些服务器的相关地址在一般的数据文件中出现的概率很大，适合进行长期观测．因此系统将对这些服务器服务之类进行长期的监测，并显示给用户看．

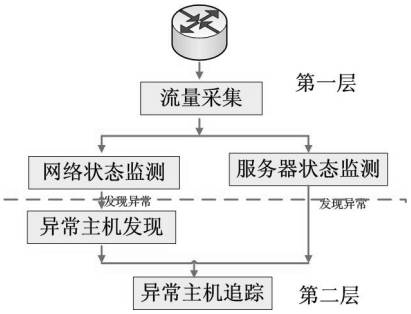

图 1　网络服务质量监测系统的流程图

第一层次是在正常情况下系统的日常工作．在发现了异常情况后，需要对异常情况进行定位，进入第二层的工作．如果网络状态监测发现了异常，需要进入异常发现模块，对这个用户群所连接的 IP 进行监测，按照一定的规则发现可能出现问题的 IP 地址，吞吐量过大或者流数过大都是可能的表现．此外在对服务器状态进行监测的过程中，如果发现状态异常的服务器，也需要进入第二层中的异常主机追踪模块．

在这个流程图中，系统得以正确运行需要几个重要的判据：①网络状态监测依赖于对网络状态的判断；②服务器状态监测依赖于对服务状态的正常和异常的判断；③异常主机的发现；④异常服务的追踪涉及到对网络状态的表达，也即将认为可能异常的服务状态表达给用户看．

3　网络服务质量监测系统中的判据

3.1　数据分析方法

数据来源为中国教育科研网某省主干网边界上采集的 Netflow 数据．按五元组（源和目标地址、端口和协议）为键值对流进行整合，认为键值相同、时间上可以衔接的为同一个流，此外 Netflow 提供的是单向流，因此在 5min 的粒度内也对流进行了双向的整合．短流的估计准确性较差，因此只需要对超过一定报文数目的长流进行分析就可以了．

3.2　单个区域的变化规律

对单个区域总吞吐量分析，发现流量变化随着一天 24h 有明显的周期规律，即总体趋势的变化是可预测的．TCP 和 UDP 流量主导了全部网络流量的 97%以上，研究网络性能问题，将重点集中在这两种网络协议上就可以满足需求．此外白天和夜间 TCP 和 UDP 报文数之比值变化较大，夜间以 TCP 报文居多，白天 UDP 报文数目略多于 TCP 报文数目．说明白天和晚上的应用类型变化很大．这些总体特征是流程图中的判断依据 1．

3.3　单个服务的服务指纹

根据进出报文数目对一天内 Netflow 流中吞吐量最大的 IP 进行排序，UDP 应用虽然是无连接的，但是在数据处理时也按照 3.1 所述方法进行流的整合．按 TCP 和 UDP 协议分成两组，分别分析其行为．发现 TCP 协议的流记录中，排名前 10 的 80%的是 HTTP 服务；UDP 协议的排名最前面的通常是 53 端口（域名服务）．由于服务器提供的服务是稳定的，明显的特征是进出报文比在一定范围内是稳定的．

由图 2 和图 3 可以看到，2 个不同服务器的出入报文比变化较平稳，对多个服务器的统计都有类似结果．由此可以认为，一个服务器在正常服务的情况下，确定的服务类型和相对稳定的内容，以及正常传输时的访问控制策略决定了出入报文比值是稳定的．这个稳定值可以作为服务器正常工作的基准值，当这个基准值发生较大的突变时，往往是出现了服务拥塞，拥塞的原因可能是链路故障或者服务器故障，包括安全攻击．图 2 和图 3 中两个服务的区别是报文比值稳定在不同的点，HTTP 服务在 1.7 左右，而 DNS 在 1.1 左右，不同的服务类型导致这个结果，但是进出报文比值就某服务的正常服务状态来说是相对稳定的．由此可以设想，就提供服务的服务器而言，虽然这个值随着各个服务类型的不同会有所不同，即使是相同的服务类型，不同服务器提供的数据资源内容不同，组织结构不同，也会导致这个比值有所变化．但是在内容、服务类型稳定的短时间内，出报文数/入报文数的比值可以认为是服务器的服务指纹，对这个值进行持

续的监测，可以有助于发现服务异常．这个值结合服务器的吞吐量规律为第 2 节中的判断依据 2．

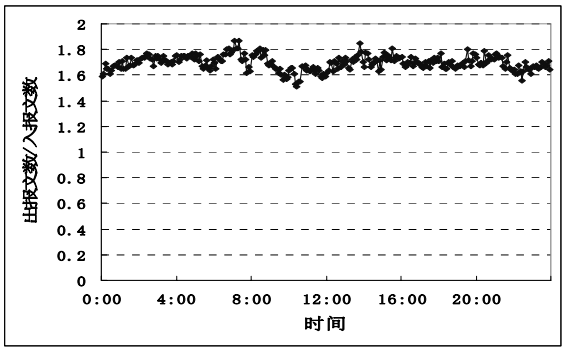

图 2　202.X.X.X:80 全天出入报文比

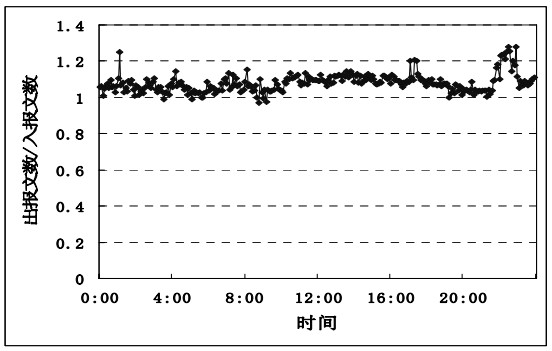

图 3　210.X.X.X:53 全天出入报文比

3.4　异常主机发现

异常的主机是指在服务器监测模块的配置之外的，引起网络异常状态的主机．这样的主机可能是一个服务器，也可能是一个用户的个人用机．最简单的方法是根据吞吐量、并发流数目的排名进行发现，结合网络安全监测的规则，可以更好的定位．

3.5　异常主机追踪

对于判断为出现异常的主机，可以使用其他的工具和数据源进行诊断，如：①使用 PING，这个方法可以快速确定延迟，但是要插入主动测量报文；②使用 RTT 与流速的经验模型进行判断，这个方法不需要主动测量，但是模型的建立比较复杂，此外在流量很小的时候，由于抽样数据求得的流速误差很大，无法使用模型进行判断，只能使用方法①；③通过服务指纹的变化，根据经验判断可能出现的问题．

4　结语

设计了一个基于 Netflow 的应用服务质量监测系统．该系统可以自适应地从历史数据中提取服务器的服务指纹作为服务质量的基准点，对当前的用户关注的服务器的服务水平给出评判，并可以通过网络的异常状态，发现导致服务质量水平下降的可疑主机并进行追踪．该系统的数据源为 Netflow 流记录，通过被动方式获得的数据源不会增加网络运行的负担，可以如实地反映网络的当前状况．服务器指纹的应用使得该系统对网络中新出现的应用具有可扩展性，有较好的应用前景．

参考文献(References)

[1] The Internet Engineering Task Force. IETF IP performance metrics work group (psamp)[EB/OL].(2008-04-23)[2008-05-30]. http://www.ietf.org/html.charters/ippm-charter.html.

[2] Cisco Systems Inc. Cisco Netflow[EB/OL]. (2007-05-22)[2008-05-30]. http://www.cisco.com/en/US/ tech/tk812/technologies_ white_paper09186a008022bde8.shtml.

[3] Zhang Yin, Breslau Lee, Paxson Vern. On the characteristics and origins of Internet flow rates[C]// Proceedings of Sigcomm. Pittsburgh ,USA, 2002:309-322.

[4] Nick Duffield, Carsten Lund, Mikkel Thorup. Properties and prediction of flow statistics from sampled packet streams[C]// Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurment. Marseille, France , 2002：159-171.

[5] Kim Myung-Sup, Yong J Won, Hong James W. Characteristic analysis of internet traffic from the perspective of flows[J].Computer Communications,2006,29(10):1639-1652.

[6] Estan C, Varghese G. New directions in traffic measurement and accounting: focusing on elephants, ignoring the mice[J]. ACM Trans on Computer Systems, 2003,21(3):270-313.