第 33 卷 第 6 期 计 算 机 工 程 2007 年 3 月
Vol.33 No.6 Computer Engineering March 2007
·工程应用技术与实现· 文章编号：1000—3428(2007)06—0245—03 文献标识码：A 中图分类号：TP393

基于 sFlow 技术的通信网络流量异常监测方案

刘国萍[1,2]，左 维[1]，李春来[1]，欧阳自远[1]
(1. 中国科学院国家天文台，北京 100012；2. 中国科学院研究生院，北京 100040)

摘 要：月球探测科学应用中心是实现嫦娥工程科学目标的基地，通信网络是其业务运行的支撑平台。该文阐述了在该通信网络环境下实施网络异常监测的必要性。提出了一种基于 sFlow 技术的具有长期效益的综合网络异常监测系统方案。
关键词：月球探测科学应用中心；通信网络；网络流量异常监测；sFlow 技术

Communication Network Traffic Anomaly Monitor Solution Based on sFlow

LIU Guoping[1,2], ZUO Wei[1], LI Chunlai[1], OUYANG Ziyuan[1]
(1. National Astronomical Observatories, Chinese Academy of Sciences, Beijing 100012;
2. Graduate School, Chinese Academy of Sciences, Beijing 100040)

【Abstract】The science and application center of lunar exploration engineering is a base for realizing the science object of Chang'e engineering while the communication network is a operation platform for the science and application center. This paper discusses the necessity of network traffic anomaly monitoring on the above constructing communication network. A comprehensive network anomaly monitoring solution with long-term benefit is proposed based on the sFlow technology for the communication network of the science and application center for lunar exploration engineering.
【Key words】Science and application center for lunar exploration engineering; Communication network; Network traffic anomaly monitor; sFlow technology

随着网络规模的日益扩大及网络应用的不断深入，网络管理对任何一个网络任务关键型单位都显得越发重要。根据网络建设的顺序，网络管理可分为网元管理(设备管理)、运行管理、性能管理和业务管理 4 个层次。目前国内的网络管理主要停留在前两个层次上，从欧美在网络管理经验上可以知道，性能管理在整个网管中是非常重要的一环[1]。与设备管理与运行管理不同的是，性能管理的资料来源主要是网络流量，这些流量可能来自内部网络也可能来自外部网络，因此通过监视透过网络出口交换设备里的输入输出流量可以较为准确及时地检测出网络性能下降和/或网络拒绝服务等网络异常的多种因素。网络异常通常是指网络偏离于非正常行为下的运行状态[2]。

随着计算机网络技术的飞速发展，网络应用急剧增长，网络病毒及攻击手段也不断翻新，由于网络性能管理不当或网络病毒等原因导致：(1)网络出现异常的机率增大；(2)定位异常点的难度加大；(3)网络异常扩散更加迅猛。因此及时而准确地定位网络异常根源、优化网络性能指标、确保网络提供畅通的数据传输与资源共享，对任何网络任务关键型企业或单位，都显得尤为重要。

1 应用中心通信网络进行网络异常监测的必要性

月球探测应用中心(简称应用中心)的通信网络共有 5 个通信节点分别位于不同的地理区域，通过光纤接入运营商的 SDH 传输网实现与其余各通信节点的双向通信。要求应用中心通信网络在不考虑线路延时的情况下能实时传输科学探测数据。

应用中心通信网络由两部分网络连接而成，一部分是各个通信结点内部的局域网，另一部分是电信运营商提供的 SDH 传输网和用户的接入部分。由于 SDH 传输网是由电信运营商管理和控制的，且 SDH 传输网在帧结构中安排了丰富的开销字节，使得其网络维护管理功能更加灵活强大，同时电信部门网络管理人员在长期实际维护过程中也积累了丰富的经验，处理网络突发异常的能力相对较高。为增强接入系统的可靠性，接入光纤拟采用双路冗余备份，接入设备也拟采用关键板卡热备。因此从用户接入部分到 SDH 传输网部分网络出现异常或故障的概率相对较小。

应用中心通信网络中的各接入结点——局域网部分，虽然其主要功能仍是提供资源共享以及相互通信，但其网络任务关键，对网络可靠性及可用性能要求较高，而这些局域网络系统由于是首次建造，网络管理系统一般会着重于常规的网络设备和运行管理，对网络性能参数突变或网络攻击造成的网络异常情况的处理经验相对较少；此外多项研究表明虽然网络外部的攻击和威胁普遍存在，但往往来自网络内部因素所造成的网络异常是无法预料也是带来损失最大的[3]。为增强应用中心通信网络的可视性、缩短网络在出现异常情况下的恢复时间，构建一套性价比合理的综合网络异常监测系统将会起到事半功倍、防范于未然的效果。

基金项目：绕月探测工程基金资助项目
作者简介：刘国萍(1973－)，女，博士生，主研方向：计算机网络通信及信息安全；左 维，博士、副研究员；李春来，博导；欧阳自远，院士
收稿日期：2006-05-22 **E-mail：**lgp@bao.ac.cn

2 应用中心通信网络异常监测系统

2.1 网络流量异常监测技术

网络流量异常监测技术根据采集方式的不同可分为：基于 SNMP 的监测技术，基于 Netflow 的监测技术，基于网络流量全镜像的监测技术。

基于 SNMP 协议直接从网络设备中收集网络流量信息，但该流量信息是根据链路层地址进行聚合的，无法反映分组中 IP 地址和端口号等信息，因此它不能提供丰富的网络监测信息；同时由于对 IP 流量的统计需要网络管理中心每隔一定时间就要向网络设备发送 SNMP 请求，当监测的网络规模较大时，就会对网络带宽及网络设备性能造成较大影响。

基于 Netflow 技术的网络监测技术虽布署容易、配置简单，但其实施前提条件是网络中交换路由器及路由设备必须能支持 NetFlow 技术，这样在进行组网设备选型或后期扩展时将受到较大限制；另外由于 NetFlow 技术是基于聚合的技术，其对路由器上的数据包测量要等到一个流结束或指定的时间间隔到达才能完成测量，因此它不能提供实时的测量信息。

基于网络流量全镜像的监测技术其原理是通过交换机等网络设备的端口镜像或者通过分光器、网络探针等附加设备，实现网络流量的镜像采集和无损复制。与前述两种方式相比，流量镜像采集的最大特点是能够提供丰富的应用层信息，但由于其采集的信息丰富，处理起来需要占用较多的资源，因此其镜像数据若直接为流量采集及分析设备所接收则会因受限于系统的处理速度而不适用于高速交换网络。

如果将上述端口镜像的数据发送到具有一定采样技术的设备中，而将采样后的数据经汇聚后采用具有广泛应用基础的 SNMP 协议导出到具有流量分析功能的设备中，便可以克服传统网络流量全镜像监测技术中由于处理复杂而不能监测较高传输速率(100Mbps)的缺点，同时又因为在镜像数据流中添加诸如端口统计及交换转发信息等内容，可以提供比基于 SNMP 的方法更为详尽的网络监测信息。本文正是基于这一思想来构建应用中心通信网络的综合网络异常监测系统的，该系统将具有对网络核心设备无依赖、数据传输速率较高且能提供丰富的网络监测信息等特点。

2.2 基于 sFlow 技术的网络流量综合监测系统方案研究

网络拥堵、拒绝服务、广播风暴等问题是影响网络可用性的主要因素，应用中心通信网络要解决上述问题，除了在网络建设阶段合理规划网络布局、优化网络设计外，还需要在运行阶段能提供一个对网络的直观全面的视图，从而准确及时地了解网络的运行状态。Foundry 与InMon公司制定的sFlow架构，提供了一种在交换网络中进行网络级实时流量监测的能力[4]，目前已成为网络设备业界公认的标准（RFC3176）。它定义了sFlow代理监视流量所用的采样机制、用以控制sFlow代理的sFlow 管理信息库（MIB）以及sFlow代理将数据转发给sFlow流量监测分析系统时所应采用的封包格式。sFlow是一种导出协议格式，它增加了关于被监视数据包的更多信息，因此从统计及监测的角度上看，sFlow提供了更为丰富的网络监测信息，而且对于流量分布的分析、流量的未来趋势、异常流量的监测、故障的发现与排除可以通过软件模块来实现。本文通过构建基于sFlow技术的sFlow数据报生成系统并结合一套sFlow流量监测分析系统来实现具有全网覆盖、实时监测功能的综合网络异常监测系统。

应用中心的各通信节点是通过专线接入而形成的广域专网，网络故障或网络异常因素主要来自各局域网内部。而应用中心总部的核心交换机将是该广域专网环境中数据包的交换中心，来自任何两相连网络的性能变化都会导致通过该交换机的流量大小和内容发生变化，因此在这里采集的网络流量具有典型性，能够充分反映各局域网内部的网络行为；另外，通过配置该交换机来实现监视其上行链路的数据流量，由于上行链路的数据流量较内部骨干网小很多，这样在后端进行网络端口流量映射、流量采集、数据存储和分析都较为容易，因此这里也是采用网络流量全镜像监测技术构建综合网络异常监测系统的适宜位置。基于上述两点可在应用中心总部的核心交换机上连接一套网络异常监测系统，通过监测其上行链路上进入和流出的数据包的相关信息便可监测应用中心总部网络内部及其余各通信节点的局域网的异常 情况。

基于 sFlow 技术的综合网络异常监测系统在应用中心通信网络中的布署如图 1。为从交换机中提取数据包信息及相关接口信息，sFlow 数据报生成系统与交换机间需要两根连线：

(1)通过在核心交换机做配置可将核心交换机的一个网口配置为镜像端口的输出口，而将 sFlow 数据报生成系统的一个端口设为接收镜像数据流的输入口，这样在这两个接口之间便可让 sFlow 数据报生成系统监视进出核心交换机上行链路的所有数据包；

(2)通过将 sFlow 数据报生成系统的另外一个普通网络接口连接到交换机的一普通网络端口，sFlow 数据报生成系统可通过 SNMP 方式来收集交换机的接口统计信息，同时通过 SNMP 方式将生成的 sFlow 数据报通过核心交换机发送到 sFlow 流量监测分析系统。

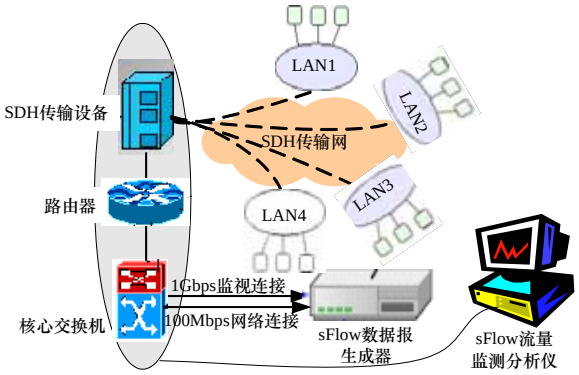

图 1 应用中心通信网络的网络异常检测系统布署图

2.3 sFlow 数据报生成系统设计

sFlow数据报生成系统完成数据包采样及sFlow数据报生成等功能，它由sFlow代理和sFlow MIB两个模块构成，如图 2。

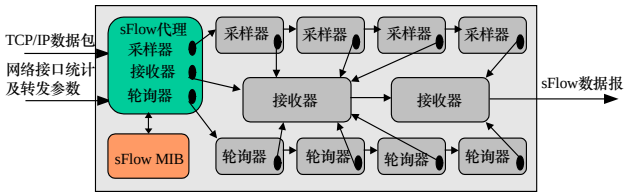

图 2 sFlow 数据报生成系统及 sFlow 代理中各模块工作流程

sFlow代理的功能是完成针对网络接口及转发表的基于时间的采样以及对IP数据包的随机采样，前者采用周期性轮询方式来对网络设备做精确的流量资料统计，它记录了与每个采样包相关的转发/路由表入口的状态。而对IP数据包的随机采样则记录了通过核心交换机传送的网络数据包信息。

2.3.1 采样相对误差

在对 IP 数据包进行随机采样时，这种取样方式在设计时必须能够保证在一个 Flow 之中所有封包都有相同的取样频率，且这种取样机制要在维持取样率的大小和准确度方面加以平衡，以保证取样后的流量能够得到有效及时的处理，又能够代表整体网络流量。

假设总共有N个数据包，从中采集n个样本进行分析，每个包被采到的概率是相同的，其中有c个指定某类型的数据包，则指定数据包的平均采样概率为P=c/n，在所有N个包中含有Nc=P×N个指定的数据包。通常假定只有当Nc的值和实际指定的包数相比误差在 5%之内这样的采样结果才具有代表性，因而也才能被接受，Nc的估计方差[5]为

$$\sigma^2 = N^2 \frac{c(1-\frac{c}{n})}{n(n-1)} \quad (1)$$

则 Nc 的置信区间是：[Nc–1.96σ，Nc+1.96σ]×%。而用错误率百分比表达则为(通常 n>>c)

$$e \leqslant 1.96 \times (1/c)^{1/2} \times \% \quad (2)$$

据式(2)可得采样相对误差如图 3，从图 3 中可以看到错误率 e 只和指定类型的采样数据包数 c 有关，当要求 e 的值小于 5 %时，c 只要大于 1 537 即可。当数据包数量庞大的时候，只要采样率根据数据包个数相应变化，使得 c 维持一个相对稳定的值，这样既能保持一定的准确度，又不会因为处理大量的数据包而大大增加系统的负荷。

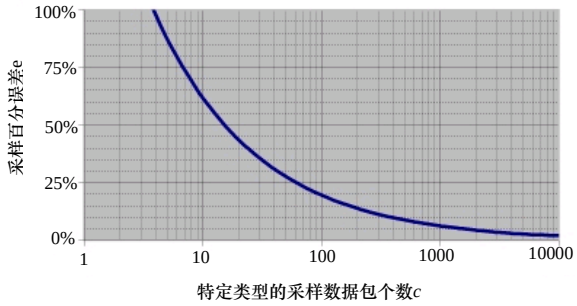

图 3 采样相对误差

2.3.2 sFlow 代理工作流程及 sFlow 数据封包格式

sFlow 代理模块由采样器、轮询器及接收器 3 个模块构成(见图 2)。在 sFlow 代理中保存了一份采样器、轮询器及接收器的链接表列，每个采样器和轮询器都有一个指向其所属的接收器的指针。通常对应于网络设备的每个接口都有一个采样器和一个轮询器，采样器负责收集包采样，轮询器负责收集接口计数器采样，而接收器用于将采样的包按 sFlow MIB 规定的结构重新编码成 UDP 数据报，输出给 sFlow MIB 指定的主机端口上的 sFlow 流量监测分析软件进行分析处理。UDP 封包格式如图 4 所示，其中 sFlow 数据报的编码格式采用了具有简单结构的 XDR 标准(RFC1155)，这使得 sFlow 代理能很方便地编码，同时 sFlow 流量监测分析系统能很容易完成解码。数据采用 UDP 包的格式在网络中传送大大减少了数据缓存量，在网络繁忙的时候能实时地传送。 由于不可靠的传送数据包会丢失，但从上面的采样机制可知，这对于采集到的交换数据流的影响是很轻微的，而丢失的接口统计数据会在下一个轮询时再次发送。

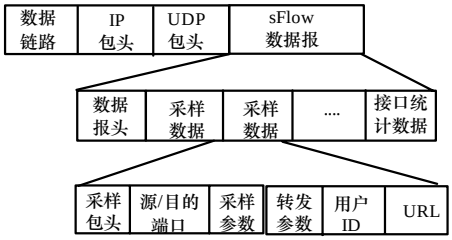

图 4 sFlow 数据报生成系统输出的数据包格式

2.3.3 sFlow MIB 架构

sFlow MIB 模块用于管理 sFlow 数据报的生成与传输，它采用 SNMP 架构。它通过 SNMP 架构里定义的标准管理机制来完成对 sFlow 代理的配置，为 sFlow 流量监测分析系统远程控制及配置 sFlow 代理提供了标准接口机制。

2.4 sFlow 流量监测分析系统设计

sFlow 流量监测分析系统用来搜集由 sFlow 数据报生成系统生成的 sFlow 数据报信息，以进行网络流量分析、趋势分析、安全分析、应用分析等。sFlow 流量监测分析系统的功能模块主要由 sFlow 数据报收集模块、数据库模块、流量分析模块、流量监测模块、应急处理模块组成。由于具有类似功能的系统市场已有相应的成熟产品，如联盈数码公司提供的综合性能分析解决方案(Integrated Performance Analysis Solution, iPerf)，设计时可根据输入数据源的不同编码格式做相应的调整。本文限于篇幅不做详细阐述。

3 结论

上述方案如在拟建的通信网络中得以正确布署，它将为网络管理者在进行网络监测时提供如下重要信息，从而可为快速而又正确地做出决策提供强有力的依据。

· 提供了良好的网络“透视”功能，使得日常网络监测工作更加透明化、综合化；

· 灵活的可扩展性；

· 较强的网络安全防范功能；

· 简易直观的操控界面；

· 合理的一次性投资。

参考文献

1 毕锦雄. 异常流量分析与网络性能管理[N]. 计算机世界(华南版), 2005-09-23.

2 Thottan M, Ji Chuanyi. Anomaly Detection in IP Network[J]. IEEE Transaction on Signal Processing, 2003, 15(5): 2191-2204.

3 InMon Corp.. Using sFlow and Inmon Traffic Server for Intrusion Detection and Other Security Application[Z]. http://www.inmon.com.

4 Phaal. InMon Corporation’s sFlow: A Method for Monitoring Traffic in Switched and Routed Networks[S]. RFC 3176, 2001-09.

5 Phaal P, Panchen S. Packet Sampling Basics[Z]. http:// www.sFlow.org.

6 杨　策. 网络流量监测技术及性能分析[J]. 空军工程大学学报(自然科学版), 2003, 4(1).