高速网络流量监测系统的设计与实现

任富新
（华北计算技术研究所，北京 100083）

摘　要：设计并实现了一种高速网络流量监测系统。该系统基于高速数据采集卡和普通服务器，在硬件采集、存储数据的基础上，实现数据捕获、分析、统计、报表等功能。通过该系统，用户可以制定针对特定业务的流量监测，并且可以对网络的健康状况和瓶颈等进行测试，帮助用户迅速地确定网络问题。目前该系统已经运行在实际网络环境中。

关键词：流量监测；端口镜像；分路器；ntop；TurboCap

中图分类号：TP393.05　　**文献标识码**：A　　**文章编号**：1674-7720(2012)01-0058-03

Design and implementation of a high-speed traffic monitoring system

Ren Fuxin
(North China Institute of Computing Technology, Beijing 100083, China)

Abstract: A high-speed traffic monitoring system is designed and implemented based on TurboCap and common server. Through the system, users can develop business-specific traffic monitoring, and acquire numerous information about network traffic, such as getting network behavior characteristics, detecting abnormal traffic, discovering network bottlenecks, locating and recovering network fault. At present, the system is running in the real network.

Key words: traffic monitoring; SPAN; TAP; ntop; TurboCap

随着互联网技术的快速发展，网络应用范围不断扩大，网络结构和网络应用越来越复杂，这使得网络出现各种问题的可能性增大，同时管理网络的难度也增大。网络流量监测提供了一种探索实际环境中网络特性的手段。从实现方法的角度，目前所存在的流量测量方法可分为两大类：基于硬件的测量方法和基于通用 PC 平台测量方法。基于硬件的测量方法由于在高速链路的环境下具有了巨大的性能优势，一般为大型开发商和运营商所用，但是因为其价格比较昂贵，大多数的中小企业还是选用基于通用 PC 的流量监测方法。然而，随着网络速率的不断提高，基于通用 PC 平台的流量监测因为受到操作系统和硬件性能的限制，不能满足高速链路流量监测的需求。

本文设计并实现了一种高速网络流量监测系统。该系统基于高速数据采集卡和普通服务器，在硬件采集、存储数据的基础上，实现数据捕获、分析、统计、报表等功能。通过该系统，用户可以制定针对特定业务的流量监测，并且可以对网络的健康状况和瓶颈等进行测试，帮助用户迅速地确定网络问题。

1 设计方案

网络流量监测验证系统由硬件支撑平台、软件支撑平台和网络流量监测应用软件（ntop）三部分构成。

1.1 硬件支撑平台

1.1.1 TurboCap 高速捕获卡

TurboCap 是一种双端口千兆捕获与注入工具，具备多种功能，包括同时全速捕获与注入、多端口通信聚合以及可调控的 pass-thru 模式。该工具套件同时提供 TurboCap API 以及 winPcap/libpcap API。TurboCap 套件包括 TurboCap 千兆捕获卡、TurboCap 驱动和用户级的 API 三部分。

1.1.2 服务器

TurboCap 卡是一种基于 PCI-E 的接口卡（4x 或 8x），为了最大程度发挥其性能，网络流量监测系统采用 HP380G6 服务器，该服务器主要配置如下：PCI-E 为 X8 PCI-E 卡插槽；CPU 采用 2.4 GHz 双核 Intel Xeon W3503；内存为 8 GB；存储为 SAS 硬盘（10 000 转）RAID 卡。

1.2 软件支撑平台

软件支撑平台主要包括 Linux 操作系统、TurboCap 卡驱动和 TurboCap Libpcap(Packet Capture Library)开发包模块等。

Linux 操作系统采用 Fedora 10，主要因为捕获卡的驱动为 Fedora 10。

1.2.1 Libpcap 开发模块

Libpcap 由 Berkeley 大学的 JACOBSON V、LERES C 和 MCCANNE S 编写，是一个平台独立的网络数据包捕获开发包，应用非常广泛，几乎只要涉及网络数据包的捕获功能，都可以使用 Libpcap 开发包。Libpcap 可以在绝大多数类 Unix/Linux 平台下工作。Libpcap 软件包可从 http://www.tcpdump.org 下载，目前最新版本为 1.1.1。

本文采用的 Libpcap 版本号为 libpcap-1.0.0-tc_17.fc10.x86_64，是由 CACE 公司提供的与 TurboCap 卡驱动配套的开发包。

1.2.2 支撑软件安装

以 ROOT 用户安装 TurboCap 驱动，TurboCap 内核模块，TurboCap 开发库、文档、例子以及支持 TurboCap 修改版的 libpcap 1.0.0，操作如下：

[root@x86_64]# rpm -ivh kernel-firmware-2.6.27.12-170.2.5.preemptive.kernel.kt.fc10.x86_64.rpm

[root@x86_64]# rpm -ivh kernel-2.6.27.12-170.2.5.preemptive.kernel.kt.fc10.x86_64.rpm

[root@x86_64]# rpm -ivh turbocap-1.6.2117-1.fc10.x86_64.rpm libpcap-1.0.0-tc_16.fc10.x86_64.rpm

[root@x86_64]# rpm -ivh turbocap-module-2.6.27.12-170.2.5.preemptive.kernel.kt.fc10-1.6.2117-1.fc10.x86_64.rpm

之后重启计算机，确认选择启动的内核是：Fedora(2.6.27.12-170.2.5.preemptive.kernel.kt.fc10.i686) 或者 Fedora(2.6.27.12-170.2.5.preemptive.kernel.kt.fc10.x86_64)

1.3 网络流量监测应用软件

ntop 是一套网络流量监控软件，由意大利 Pisa 大学教授 DERI L 于 1997 年开始开发，并以开源方式提供使用，可以从 http://www.ntop.org 下载，目前最新版本为 4.0.3。ntop 以 sniffery 方式运作，采用网页接口，主要功能有网络监控、网络流量统计、提供网络最佳化与除错的信息以及侦测可疑的网络流通信息等。

1.3.1 ntop 功能

ntop 可以监测的数据包括：网络流量、使用协议、系统负载和端口情况等。

ntop 能够更加直观地将网络使用量的情况和每个节点计算机的网络带宽使用详细情况显示出来。可以通过分析网络流量来确定网络上存在的各种问题，如瓶颈效应或性能下降；也可以用来判断是否有黑客正在攻击网络系统。如果怀疑网络正在遭受攻击，通过 ntop 截获的数据包可以确定正在攻击系统的是什么类型的数据包，以及它们的源头，从而可以及时地作出响应，或者对网络进行相应的调整，以保证网络运行的效率和安全。通过 ntop 网管员还可以很方便地确定哪些通信量属于某个特定的网络协议、占主要通信量的是哪个主机、各次通信的目标是哪个主机、数据包发送时间、各主机间数据包传递的间隔时间等。这些信息为网管员判断网络问题及优化网络性能，提供了十分宝贵的信息。

1.3.2 ntop 基本架构

ntop 基本架构分成三个模块：数据包捕获(Packet Sniffer)模块，数据包分析(Packet Analyser)模块以及报告引擎(Report Engine)模块，如图 1 所示。由 Packet Sniffer 收集网络上的 Packet，然后送给 Packet Analyser 去处理，再由 Report Engine 将处理分析后的数据呈现出来。

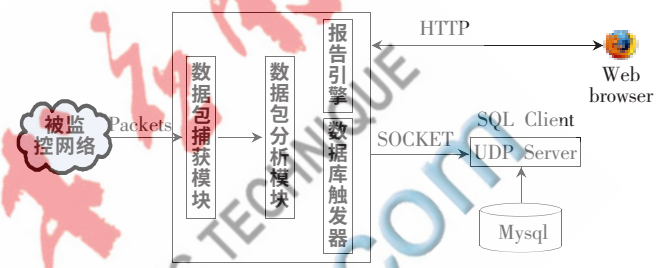

图 1 ntop 的基本架构

1.3.3 ntop 安装与使用

在 FC10 下，ntop 的安装配置更简单，大多数库默认都已经安装，只需另外安装 GeoIP 和 rrdtool，下面简单介绍一下 ntop 的安装和配置。

解压缩源码：tar -zxvf ntop-4.0.3.tar.gz；

运行：cd ntop-4.0.3；

运行：./autogen.sh；

运行：make && make install；

添加用户：useradd -M -s/sbin/nologin -r ntop；

设置用户权限：chown ntop:root /usr/local/var/ntop/；

设置用户权限：chown ntop:ntop /usr/local/share/ntop/；

设置密码：ntop-A；

ntop 作为守护进程运行：/usr/local/bin/ntop -d -L -u ntop -P/usr/local/var/ntop --skip -version -check --use-syslog=daemon；

查看统计信息：打开浏览器，在地址栏输入 http://host_ip:3000(“IP”就是安装 ntop 的那台网管工作站的 IP 地址)，即可打开 ntop 界面。

2 网络流量监控系统的接入方式

2.1 网络数据获得技术

在交换网络中，有两种有效的获得数据的方法：

(1)镜像端口 SPAN(Switch Port Analysis)：某些交换机可以将一个或几个端口的数据包复制到一个指定的端口，然后可以在该端口上接网络流量监测系统。

(2)分路器 TAP(Test Access Port)：可以把任意一个端口收到的数据注入到另一个端口。可用于即时分析网络流量，且不占用任何网络资源。分路器 TAP 串接在

被监控链路上，可永久固定在被监控链路上，避免插拔链路，不用配置交换机和额外占用交换机端口。

2.2 网络流量监控系统的部署方式——SPAN 方式

网络流量监控系统的部署方式为 SPAN 方式。下面主要说明如何在 Catalyst 2950 上配置 SPAN 功能，以下是 SPAN 实现的范例：

```
C2950#conf t
C2950(config)#
C2950 (config)#monitor session 1 source interface fastEthernet 0/2
! -- Interface fa 0/2 is configured as source port
C2950 (config)#monitor session 1 destination interface fastEthernet 0/3
! -- Interface fa0/3 is configured as destination port
C2950(config)#
```

在使用 SPAN 时需要注意：(1) 保证镜像端口的线速等于或高于被监测端口的线速，防止数据过载，造成数据包丢失；(2)SPAN 功能会增加交换机的负荷，占用交换机的 CPU、内存等系统资源，致使交换机性能下降，所以在获取到足够的数据后，需要去除 SPAN 功能；(3) 由于不同交换机转发机制不同，有的交换机的 SPAN 功能会自动丢弃错误的数据包，导致无法获取到错误的数据包，而错误的数据包能为解决网络问题提供重要依据。

2.3 网络流量监控系统的部署方式——TAP 方式

网络流量监控系统的部署方式采用 TAP 方式，TAP 方式又分以下几种：

(1) 交换分路器（TAP）模式。当 TurboCap 卡处于 pass-thru 模式时，TurboCap 把一个端口收到的数据注入到同卡上的另一个端口。两个端口支持全速对发，从而使 TurboCap 具有分路器的功能。

(2) 汇聚 TAP 模式。安装方法类似于交换 TAP。汇聚 TAP 可以将多条链路的全双工数据合并到单一数据流中，这样可以从单一数据流中看到来自多个 SPAN 端口的汇聚流量，将其复制后供分析使用。TurboCap 支持同卡上的全速双口通信聚合。用户可以通过一个叫做 Board Aggregationg Port(BAP) 的虚拟端口来访问聚合通信。TurboCap 还支持对多 TurboCap 卡的端口进行聚合，这样用户可以一次捕获超过两个端口的通信。

在借助 TAP 分析网络数据的时候，需要注意以下三点：(1)TAP 主要用于对骨干链路数据的获取（当然也可以用于其他链路），使用时需要预先布放（串接）到链路中，避免监测骨干链路时再串接 TAP 而引起中断网络的情况发生；(2) 被监测的链路流量不要超过 TAP 端口的线速，防止数据包因过载而丢失；(3) 将不同的 TAP 组合起来使用可以实现更高要求的数据监测，通过 TAP 模式和聚合功能，就可以实现聚合 TAP 的功能。

本文基于高速采集卡和普通服务器设计了高速网络流量监测系统，采用 Linux 操作系统和开源软件，成本低，满足了高速链路流量监测的需求。该系统既支持 SPAN 方式，也支持 TAP 方式，这两种技术在网络监测、分析时都普遍应用。用户可以根据自己的使用情况，选择合适的部署方式来部署网络流量监测系统。

参考文献

[1] 郑惠之，罗进文. 一种有效的流量控制策略—ntop[J]. 信息科技，2002(3)：38-39.
[2] 赵冉. 网络流量测量系统 Ntop 的分析与研究[D]. 西安：西北大学，2008.
[3] TAMON M A. Ntop network monitoring guide [EB/OL]. [2008].http://techowto.wordpress.com.

（收稿日期：2011-08-02）

作者简介：
任富新，男，1974 年生，硕士研究生，工程师，主要研究方向：嵌入式系统、网络性能测试。