# 中心计算机网络流量监测系统的研究与实践

朱 珺
(92941 部队 96 分队，辽宁 葫芦岛 125000)

**摘 要**：研究并解决网络流量监测中的各种关键技术，提出符合中心计算机系统实际情况的网络流量监测系统的架构；设计并实现了网络流量监测系统，该系统基于 Turbocap 千兆捕获卡和工作站。通过该系统，用户可以制定针对特定业务的流量监测，并根据详细的流量信息实现故障定位。目前该系统已经运行在中心计算机系统网络中。

**关键词**：网络流量监测；Libpcap；ntop；span；tap；TurboCap
**中图分类号**：TP393.05 **文献标识码**：A **文章编号**：1674-7720(2013)12-0054-03

## Research and practice of center computer network traffic monitoring system

Zhu Jun
(96 Detachment of 92941 Troops, Huludao 125000, China)

**Abstract**: Study and solve the network traffic monitoring of various key technology, put forward accord with the actual situation center computer system architecture of network traffic monitoring system; Designed and implemented the network traffic monitoring system, whitch based on TurboCap and workstation. Through the system, users can develop business-specific traffic monitoring, and in accordance with the detailed traffic information to realize fault location. At present, the system is running in the center computer system network.

**Key words**: network traffic monitoring; Libpcap; ntop; span; tap; TurboCap

## 1 系统概述

中心计算机系统是武器试验靶场测控系统中数据处理与转发的枢纽，是典型的实时系统，主要任务是综合接收、实时处理各种测量设备信息。随着网络技术的发展，中心计算机系统由点对点的专用通信链路(HDLC、串口)向网络通信过渡。整个测控系统的 IP 化是必然趋势。将来，所有的测控设备都必需提供 IP 接口，以 IP 数据包交换为特征的网络通信会逐步替代以点对点为主的传统通信方式。随着基地网络应用范围的不断扩大以及网络的日益复杂化，网络管理工作的难度也越来越大。因此根据基地网络实际情况设计了一种网络流量监测系统，用来测试中心计算机系统网络的性能和可靠性。通过该系统，可以对网络的健康状况与瓶颈进行测试，迅速地确定网络问题。

### 1.1 研究目的

本课题的研究目的是以中心计算机系统为应用背景，研究并解决网络流量监测中的各种关键技术，提出符合中心计算机系统实际情况的、技术可行的网络流量监测系统的架构和应用方式，并构建一套可满足中心计算机系统应用的网络流量监测系统。

### 1.2 研究意义

网络流量监测有助于维护网络持续、高效和安全地运行，网络流量监测的意义在于取得对网络运行管理、应用运行管理和网络问题分析有意义的数据。这些数据(包括利用率、b/s、pps、网络延迟、重传、连接数量等)只有与实际的网络应用运行情况结合起来才有意义。这是因为不同的网络、不同的应用都有完全不同的数据流量。只有对网络和应用进行深入地了解，才能使这些数据的价值得到真正的体现。网络流量的监测对于技术人员了解网络、发现问题、确认问题原因有着重要的意义[1-3]。

## 2 方案设计

网络流量监测从不同的方面可以分为如下几部分：

(1)基于硬件探针的测量和基于软件的测量

基于硬件探针的测量通常指使用专用硬件设备进行网络流的测量，捕获和实时分析能力强，但一般价格昂贵。基于软件的测量通常是在 PC 上安装软件来实现。与基于硬件的方法比较，费用比较低廉，但是性能一般。

(2)主动测量和被动测量

主动测量使用由测量设备产生的数据流来探测网络而获知网络的信息。被动测量只是记录网络的数据流,不向网络流中注入任何数据。大部分网络流量测量都是被动测量[4-5]。

(3)在线分析和离线分析

在线分析指实时地收集和分析网络数据,同时显示流量数据和分析结果。离线分析只是在线地收集网络数据并存储下来,并不对数据进行实时的分析。

(4)协议级分类

对于不同的协议,例如以太网(Ethernet)、帧中继(Frame Relay)、异步传输模式(ATM),也就有了不同的通信量测试方法。

根据中心计算机网络的实际情况,采用基于硬件测量方式、被动在线测量以及针对以太网的协议。经过充分调研和分析,基于高速数据采集卡(TurboCap)和工作站来构建流量监测系统,采用 Linux 操作系统和开源软件(LibpCap、ntop)来实现流量监测功能。

## 2.1 硬件系统

### 2.1.1 TurboCap 千兆抓包卡

TurboCap 卡是一种基于 PCI-E 总线的高速抓包卡,提供 TurboCap API 以及 LibpCap API[6]。如图 1 所示。

图 1 TurboCap 千兆抓包卡

### 2.1.2 计算机配置

为了保证抓包速度,需要计算机具有 PCI-E 8x 插槽,8 GB 以上内存。

## 2.2 软件系统

软件系统主要包括 Linux 操作系统、TurboCap 开发套件、LibpCap、ntop 等。

### 2.2.1 LibpCap

LibpCap 是一个平台独立的网络数据抓包开发包,其应用非常广泛,可以在绝大多数类 Unix/Linux 平台下工作,提供了用户级 API 编程接口,并充分考虑到应用程序的可移植性。LibpCap 隐藏了操作系统的细节,为底层网络监控编程提供一个易于移植的应用框架,可以捕获网络上的所有数据包。

### 2.2.2 TurboCap 开发套件

TurboCap 开发套件包括 TurboCap 驱动、TurboCap 内核模块、用户级的 API 以及 TurboCap 开发库、文档、例子。

### 2.2.3 网络流量监测软件 ntop

ntop 可以从 http://www.ntop.org 下载,并以开源方式提供使用,是 Linux 下著名的网络流量监测软件。ntop 是一种网络嗅探器,以 sniffery 方式运作,可以监测的数据包括:网络流量、使用协议、系统负载、端口情况等。ntop 能够显示基于 IP 地址的带宽占用情况,帮助技术人员迅速定位占有大量带宽的主机和应用,还能基于协议的类型进行统计并生成直观的图表,帮助技术人员了解业务流量的组成和比例,进而以此为依据来优化网络。

在使用 ntop 的过程中,解决了一些问题,主要包括:

(1)在没有连接互联网的情况下 ntop 无法编译安装;

(2)在对 ntop 的源码编译时提示没有定义 pthread_mutex_trywrlock;

(3)ntop 运行过程中会出现拒绝远程的连接请求等。

此外还对 ntop 进行了一些改进,包括对历史数据的保存、数据导出等。为了用户使用方便,对 ntop 的 Web 界面显示进行了汉化,主要是修改 http.c 和 report.c 两个文件。

## 2.3 关键技术研究

中心计算机网络流量监测系统的关键技术包括如下几种。

### 2.3.1 千兆以太网线速抓包技术

在搭建网络流量监测系统时需要全速千兆以太网抓包,这绝对是一项挑战性任务。采用通用的设备,如何做到捕包性能最好、不丢包,是需要突破的关键技术。而采用纯软件的技术是无法达到线速抓包的,因此必须由硬件来配合。为了提高抓包性能,采取了以下措施:

(1)采用高端配置的工作站或者服务器,包括配备带缓存的磁盘阵列、高速 SAS 硬盘,CPU 和内存也要考虑配得高一些;

(2)采用高速抓包卡(TurboCap),用 TurboCap 自带的测试程序 HighSpeedTransmitter、HiPerfPktReceiver 进行收发包,用思博伦的 Smartbits 测试,TurboCap 可以达到线速。

### 2.3.2 数据包获得技术

在交换网络中,有两种获得数据的方法:

(1)端口镜像 SPAN(Switch Port Analysis)。简单来说就是把交换机某个端口的流量 copy 一份到另外一个端口,然后可以在该接口上接网络流量监测系统。

(2)分路器 TAP(Test Access Port)。需要串接在被监测链路上。

中心计算机网络流量监测系统既支持 SPAN 方式,也支持 TAP 方式。这两种技术在网络监测、分析时普遍应用,每一种技术都有其优点和缺点:

(1)SPAN 比较灵活,无其他设施需求,无需改变网络拓扑结构;而 TAP 则需要接入到链路中去,如果需要监测其他的链路,则需要重新连接线缆,会对网络造成中断,适合长期的稳定监测。

(2)SPAN 需要对交换机进行配置,占据一个交换机端口;而 TAP 没有这个问题,它对于网络设备来说是透

明的，不干涉数据流和原始数据；

(3)SPAN 方式获得的流量其实已经被过滤掉一些底层的信息了，所以有些故障信息无法看到，而 TAP 真实反映了网络的流量，没有任何修改；

(4)SPAN 只适用于交换机，如果需要监测的链路两端都是路由器，就无能为力了；而 TAP 这方面就没有任何问题。

2.3.3 网络流量监测系统接入方式

由于受到网络结构、网络技术、网络设备、传输线路和用户应用等多种条件的限制，如何将网络流量实时监测系统在不影响网络应用的前提下，快速、准确、安全地连接到被测网络中，成为一个具有挑战性的问题。网络流量监测系统的部署方式有多种：

(1)并接，即 SPAN 方式。将交换机一个端口的数据包复制到一个指定的端口，然后可以在该接口上接网络流量监测系统，即 TurboCap 卡的一个接口。

(2)聚合模式。对两个千兆网口进行聚合，按照时间戳记对来源于不同位置的数据进行采集、分析，该模式可用于测量不同位置网络包的延迟。

(3)串接，即 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。只是 TurboCap 在 pass-thru 模式下与普通 TAP 的连接性不同：装有 TAP 的计算机必须开机正常运行，如果关机，处于 TAP 位置的通信将中断。

(4)汇聚 TAP 模式，类似串接 TAP。汇聚 TAP 可以将一条或多条链路的全双工数据合并到单一数据流中供分析，这样能够在单一数据流中看到来自多个端口的汇聚流量。

2.3.4 用户特定业务流量监测

中心计算机有很多非标准的网络应用。对于用户来说，在进行网络流量监测时，如果能灵活定义需要监测和分析的业务，可快捷地找到网络故障与问题，从而提高解决问题的效率。在 Linux 操作系统下，文件“/etc/services”保存的是 Internet 服务和与之对应的端口号。该文件的每一行描述了一种服务，格式为：

service-name port/protocol [aliases ...]

其中 service-name 是服务的名字；port 是十进制的数字，用来代表该服务；protocol 是使用的协议类型，典型的值包括 tcp 和 udp；aliases 是可选的代表该服务的别名。

通过 services 文件，用户可以设置自己的应用，例如：

中心机接收端口 8201/udp

这样，就很容易区分用户不同的服务。

2.4 应用举例

中心计算机网络流量监测系统可以监测的数据包括：网络流量、使用协议、系统负载、端口情况、数据包发送时间等，能够显示基于 IP 地址的带宽占用情况，还能基于协议的类型进行统计并生成直观的图表，将每个节点计算机的网络使用详细情况显示出来；还可以很方便地确定出哪些通信量属于某个特定的网络协议、占主要通信量的主机、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。下面介绍两个简单的使用例子。

(1)举例一

选择“全部网络协议”→“流量”菜单选项，在 Hosts 下拉列表框中选择 Local Only，在 Data 下拉列表框中选择 Received Only，在 Data 栏上单击，对数据和百分比进行排序。可以很容易地发现当前网络中接收带宽的最大占用者。

如果想知道当前网络中发送带宽的最大占用者，在 Data 下拉列表框中选择 Sent Only 即可。

(2)举例二

选择“网络层协议统计”→“本地”→“本地矩阵”菜单选项，就可以看到本地主机发送的数据矩阵，找出发送数据最多的主机。

中心计算机网络流量监测系统基于 TurboCap 千兆捕获卡和普通工作站设计，简单实用，性价比高；采用 Linux 开源操作系统和开源软件(LibpCap、ntop)，安全性高。中心计算机网络流量监测系统自动从网络中识别有用的信息，直观地呈现给技术人员；将截获的数据包转换成易于识别的格式，使技术人员一目了然；该系统基本满足中心计算机系统大多数网络流量监测的需求，大大提高了网络的利用率。

中心计算机网络流量监测系统还存在一定的不足，主要表现在：虽然 TurboCap 高速捕获卡支持线速抓包，但是 ntop 通过 LibpCap 接口对 TurboCap 高速捕获卡操作时，由于 LibpCap 的性能问题，无法达到线速抓包；ntop 的远程访问还存在安全方面的问题。因此还需要对中心计算机网络流量监测系统进行改进。

参考文献

[1] 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.

[2] 任富新.高速网络流量测量系统的设计与实现[J].微型机与应用，2012，31(1)：58-60.

[3] 沈华林.协议/流量分析系统 Hntop 的实现[J].计算机工程与应用，2005，41(16)：137-139.

[4] TAMON M A.Ntop network monitoring guide[EB/OL].[2008-05-25].http://techowto.wordpress.com.

[5] 夏光峰.网络分析技术及其在网络管理中的应用研究[J].电脑知识与技术，2009，5(3)：587-590.

[6] Riverbed.CACE turbocap_flyer[EB/OL].[2010-01-18].http://www.cacetech.com.

(收稿日期：2013-03-16)

作者简介：

朱珺，男，1969 年生，本科，主要研究方向：武器飞行试验测控应用软件技术、计算机网络。