学校编码：10384　　分类号_____密级_____
学号：22120051302290　　UDC _____

厦门大学

硕 士 学 位 论 文

Linux 环境下基于 Intel 千兆网卡的高速数据包捕获平台的研究

The Research of High-Performance Packet Capture Platform Based on Intel Gigabit Network Card in Linux Environment

刘 峰

指导教师姓名：黎忠文 教授

专 业 名 称：计算机系统结构

论文提交日期：2008 年 5 月

论文答辩时间：2008 年 月

学位授予日期：2008 年 月

答辩委员会主席：_____

评 阅 人：_____

2008 年 5 月

厦门大学学位论文原创性声明

兹呈交的学位论文，是本人在导师指导下独立完成的研究成果。本人在论文写作中参考的其他个人或集体的研究成果，均在文中以明确方式标明。本人依法享有和承担由此论文产生的权利和责任。

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人完全了解厦门大学有关保留、使用学位论文的规定。厦门大学有权保留并向国家主管部门或其指定机构送交论文的纸质版和电子版，有权将学位论文用于非赢利目的的少量复制并允许论文进入学校图书馆被查阅，有权将学位论文的内容编入有关数据库进行检索，有权将学位论文的标题和摘要汇编出版。保密的学位论文在解密后适用本规定。

本学位论文属于

1、保密（　），在　　年解密后适用本授权书。

2、不保密（　）

（请在以上相应括号内打“√”）

作者签名：　　日期：　　年　月　日

导师签名：　　日期：　　年　月　日

摘　要

线速地实时处理网络报文流是入侵检测系统、网络协议分析、网络防火墙、高性能通信系统、高性能路由器、主机路由器，以及其他网络监视系统必须满足的首要条件。

当前大部分的入侵检测系统、防火墙等网络监视及防御系统都是基于运行在 PC 架构上的 Linux 平台。

百兆的网络环境下，普通的网卡和 Libpcap 接口就足以保证运行在 Linux 用户空间的网络报文处理程序线速地捕获网络报文。如：tcpdump、ethereal 和 snort 等程序。然而千兆网络时代的到来，使得在通用操作系统下远达不到线速捕获网络数据包。本文实现了一种高性能的网络数据包的捕获平台，省去了数据包在内核和用户空间传递过程中的拷贝，缓存，以及系统调用过程，从而使得网络报文的处理性能有很大提升。

本人主要工作如下：

1．对 Linux 网络协议栈进行了分析，并对传统报文捕获平台 Libpcap 进行了分析研究。

2．深入分析了 Intel 千兆网卡驱动及相关的中断机制，软中断机制及内存映射机制。

3．在深入分析 Linux 2.6 内核的基础上，实现了一种新的基于 Intel 千兆网卡的高性能的网络数据包捕获平台 ZeroP。ZeroP 由两部分组成，一部分是位于内核空间的驱动模块，另一部分是用户空间的兼容 Libpcap 的接口。

4. 搭建了 CISCO 测试平台，对 ZeroP 平台进行了性能及兼容性测试，并对测试数据进行了分析。

关键字：NAPI；中断；E1000 网卡驱动；Mmap

Abstract

Many network monitoring systems are based on wire-speed packet capture and real-time analysis. Such as, intrusion detection systems, protocol analysis, network firewall, high-performance communications systems, high-performance router, host routers and other network monitoring systems.

At present, most of the intrusion detection system, firewall, and so on are based on PC architecture running on the Linux platform.

In fast network environment, the common interface card and Libpcap is enough to guarantee that the user space application, on the linux system, can wire-speed capture network packets.such as: tcpdump, ethereal and snort, and so on. As the time of the gigabit network, it is impossible for general operating system to capture packet or send packet at wire speed. This paper designs a high-performance zero-copy platform, it decreases the number of the copy and the buffer between kernel and user space, reduces the overhead of the system call, thus the network packet processing performance is greatly improving.

Main tasks:

1. Analysed the Linux network protocol stack, analyzed the traditional packet capture platform Libpcap.

2. Analysed the Intel Gigabit Ethernet driver deeply, the interrupt mechanism, the soft interrupt mechanism and the memory mapping mechanism.

3. We implemented a new high-performance network packet capture platform ZeroP based on Intel-based Gigabit Ethernet in the Linux 2.6 kernel. The ZeroP platform contains two components: a device driver module in kernel-space and a user-space library compatible with Libpcap.

4. Built CISCO test platform, tested the performance and the compatibility, analysed the test data.

Key Words： NAPI; Interrupt; E1000 driver; Mmap

目 录

Contents