研究报告

嵌入式无线接入点网络驱动的设计与实现

王质礼，胡爱群，宋宇波

（东南大学信息安全研究中心，南京 210096）

[摘要] 分析了嵌入式 Linux 系统下网络驱动的体系机构和工作原理，结合 PCMCIA 驱动接口，着重论述了嵌入式 Linux 无线接入点网络驱动的基本软件模型和实现流程，给出了网络驱动的性能测试结果。

[关键词] 嵌入式 Linux；网络设备驱动；PCMCIA

[中图分类号] TP393.17 [文献标识码] A [文章编号] 1009－1742（2005）10－0091－04

1 引言

随着网络、通信、芯片等技术的发展，嵌入式应用设备的数据处理、信息传递、用户交互等都对操作系统的网络功能提出越来越高的要求。现在流行的嵌入式操作系统主要有 VxWorks，WindowsCE，QNX Nutrino 等，但大多数只有简单的网络通信功能。Linux 操作系统作为遵循 GPL，源代码开放，专门为网络环境编制的操作系统，广泛应用于嵌入式系统开发领域。Linux 将通信和网络功能和系统内核紧密结合，内置灵活的联网特性，是当前对网络协议支持最全面的操作系统之一。因此，网络设备驱动程序的开发是嵌入式 Linux 系统设计与开发的重要部分。

网络设备驱动是整个网络体系结构的基础，它通过物理设备读取和发送报文，为上层网络协议和物理设备间架设桥梁。笔者结合嵌入式设备无线接入点（access point）的开发，介绍嵌入式 Linux 网络设备驱动程序的设计和实现，以及基于 PCMCIA 接口的 AP 系统网络驱动开发流程。

2 Linux 网络驱动体系结构及 PCMCIA 网卡驱动接口

Linux 网络设备驱动体系结构[1]可分为 4 层，如图 1 所示，从上到下分别为：网络协议接口层、网络设备接口对象、网络设备驱动功能层及网络设备与介质。信息传输必须通过这 4 部分协调来完成。在 Linux 系统中，用 Device 数据结构独立抽象每个网络设备接口来完成与硬件交互作用，全部网络设备接口组成一个以 dev_base 为指针的设备链表。在系统初始化的最后，剩下来 dev_base 内的所有节点全是系统检测到的网络设备。协议接口层隐藏了网络设备驱动程序的实现细节，为上层协议层提供统一的抽象接口服务。相邻层通过 dev_queue_xmit，netif_rx 等特定函数调用，透明了数据通信过程。因此，网络驱动程序的设计，关键是网络驱动功能层的具体实现。网络驱动功能层又包括初始化（探测物理设备、配置资源、初始化 Device 结构、注册设备）、数据包接收和数据包发送（hard_start_xmit 函数指针是和某一种具体的硬件相关的，通过 dev_queue_xmit 这个外部函数，调用该函数指针来完成网络数据的发送过程）3 个主要功能模块。

Linux 内核中 PCMCIA 驱动[2]由 Driver Services，Card Services，Socket Driver 三部分组成，如图 1 所示，Driver Services 通过注册函数 register_pccard_driver 为 Card Services 与驱动开发

[收稿日期] 2004－09－14；修回日期 2004－12－16

[基金项目] “八六三”高技术开发计划资助项目（2003AA143040）

[作者简介] 王质礼（1980－），男，江苏通州市人，东南大学无线电系硕士研究生，从事通信信号处理及无线网络通信方向的研究

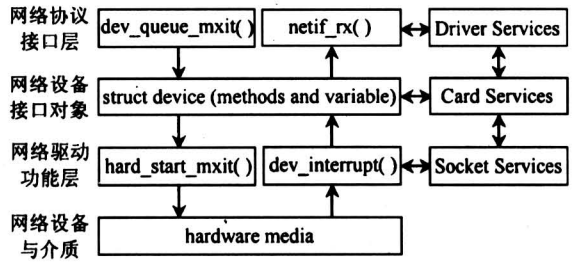

图1 Linux网络设备驱动体系结构

Fig.1 Linux network driver architecture

调用提供桥接。Card Services模块为每个特定设备（称为客户端）定义并初始化结构client_reg_t，通过Linux内核Card Services系列函数建立Card Services、客户端驱动及其客户端套接口的映射关系，实现资源配置、中断申请、I/O控制等功能，并且设置Client Event Mask，为网卡插入、重启、挂起等事件提供中断句柄处理函数。Socket Driver模块为Card Services的实现提供具体底层函数，通常这些都是由Linux内核源码来实现，复杂性比较高，驱动开发者只需调用Socket Driver模块封装的API函数接口。

3 AP系统网络驱动的设计与实现

无线接入点（access point，简称AP）[3]是负责移动终端的管理以及协调无线和有线网络之间通信的关键部件，它为在子网间漫游的移动终端提供无缝的、高速的、透明的接入服务。AP系统硬件平台采用MPC852T嵌入式Linux平台，基于16 b PCMCIA标准接口，采用内置MAC（media access control）层处理芯片的DWL－650 PCMCIA网卡，实现物理层最高11 Mb/s传输速率。开发AP网络驱动程序除了要考虑硬件驱动模块以外，还必须考虑到基于二层的AP驱动协议与上下层协议接口、无线链路与有线链路的桥接等问题。

AP实际上是一种网桥，作为无线局域网的中心，实现无线网络和以太网的有机结合，负责数据的接收和转发。嵌入式Linux实现了完善的TCP/IP协议，因此，AP网络驱动开发的根本是基于PCMCIA接口建立标准无线网络设备wlan0。AP驱动程序的实现采用Linux特有的、非常灵活的模块加载，将PCMCIA网络驱动（ap_cs.o）和IEEE802.11b MAC层协议栈（ap.o）以及数据加解密（ap_crypt_wep.o）分别作为独立的模块，动态加载。下面分别对AP网络驱动功能实现进行深入分析。

1）*初始化模块* 当用户插入网卡，系统动态加载ap_cs.o模块，模块初始化流程如图2所示。通过register_pccard_driver注册对应的client_reg_t结构，并定义事件处理句柄apClient_event负责处理网卡由Event Mask预定义的触发事件，句柄处理函数调用apClient_config，读取CIS（card information structure）信息，校验、配置资源，根据配置属性申请中断线，注册中断句柄，分配IO端口等初始化历程。如图1所示的网络驱动体系结构定义并初始化结构dev，探测物理硬件接口，用探测到的设备值填充dev结构成员（open、do_ioctl、hard_start_xmit等），完成建立标准无线设备wlan0。同时为无线网卡接收、发送数据做好准备。

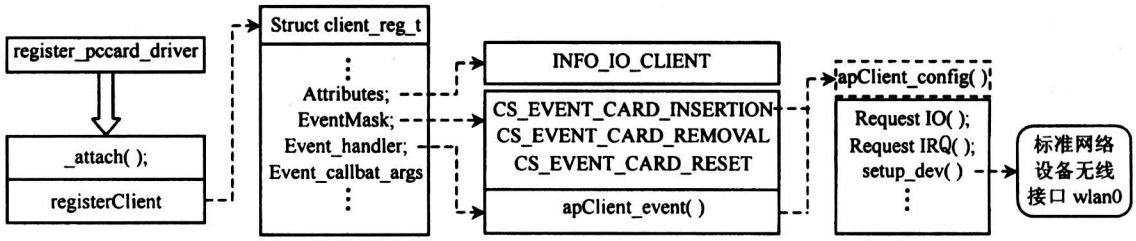

图2 CS驱动开发流程图

Fig.2 Development procedure of CS driver

2）*数据接收、发送模块* 嵌入式Linux系统中，网络设备接口以中断处理程序的方式控制，网络设备数据接收函数就是网络驱动程序的中断处理函数（即初始化时注册的中断句柄函数）。无线设备驱动中，当数据到达引起中断时，主机通过BAP（buffer access path）读取数据，调用处理程序ap_rx_tasklet进行处理，再根据中断类型，调用相应子处理程序做相应处理。如图3所示，在接收到完整的MSDU（MAC Service Data Unit）后，经校验无误，交由MAC层协议栈分析

IEEE802.11 帧头，根据源地址，建立或查询客户端 sta 对应信息的 hash 列表，如数据加密则根据对应加密算法和密钥解密数据，同时填充待转发的 skb 结构信息。如目的地址为该 AP 连接中的客户端时，则填充 skb 结构后直接调用 dev_queue_xmit 处理，调度 schedule_task，最终从无线设备接口发出。否则调用 netif_rx 转发上层，最终根据目的地址将数据包从以太网发到网络上。为了提高数据传输效率，普通数据帧都由内核直接处理，但为了便于用户态对系统认证和加密的管理，可将 802.1x 等特殊数据帧或管理帧转发至用户态，再由用户态分析处理，通过 TCP/UDP 预定端口发送到指定认证服务器。

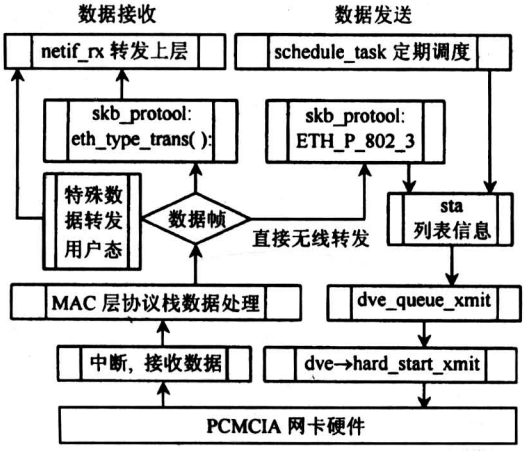

图 3　AP 网络驱动接收、发送数据流程图

Fig.3　Rx/Tx procedure of AP network driver

无线网络设备发送数据包过程则相对简单，系统定期调度 tx_exc_tasklet ( )，接收数据经合法化分析，查找客户端 hash 列表信息后，dev?hard_start_xmit 函数将间接字缓冲区链入网络设备结构管理的发送队列，唤醒网络设备，通过无线设备将队列中的数据包分别发送至对应的客户端。

3) *有线与无线链路桥接模块*　在 Kernel 2.4 及其更高版本的 Linux 内核中，以太网网桥模块有了较完善的支持。网桥在整个桥接局域网中的作用是有目的地转发数据帧。网桥数据库反映桥接局域网的拓扑结构，把从一个端口收到的数据帧按照一定的原则进行转交或过滤操作。转交过程（forwarding process）、学习过程（learning process）和相关的过滤数据库（filtering database）完成后，无线接入点成功采用网桥设备 br0 将以太网设备 eth0/eth1 和无线网络设备 wlan0 进行桥接，而以网桥设备 br0 作为与其他网络设备进行通信的唯一网络地址。

4　AP 网络驱动性能测试

由于嵌入式系统运行环境所限，必须要求系统能够稳定高效的长时间运行。为了测试基于 PCMCIA 接口开发的 AP 系统网络驱动性能，在系统开发完成后期，采用 Charito 网络战车进行了点对点/点对多点、长时间、大量重负荷的系统测试。Charito 网络战车是一个由 Chariot 控制台和 Endpoint 组成的优秀软件测试工具。它具有灵活的设计测试结构，对网络全方位进行测试。通过对测试环境、测试拓扑、运行参数等设置，分别最终得出了对无线接入点吞吐量、响应时间的测试结果，如图 4 所示。其中数据通信平均吞吐量达到 5.5 Mb/s，平均测试响应时间为 0.145 s，性能均优越于市场同类产品。该无线接入点在多终端、数据加密通信的环境下仍然保持其优越性能，其各项良好的性能进一步肯定了嵌入式网络驱动的成功开发。

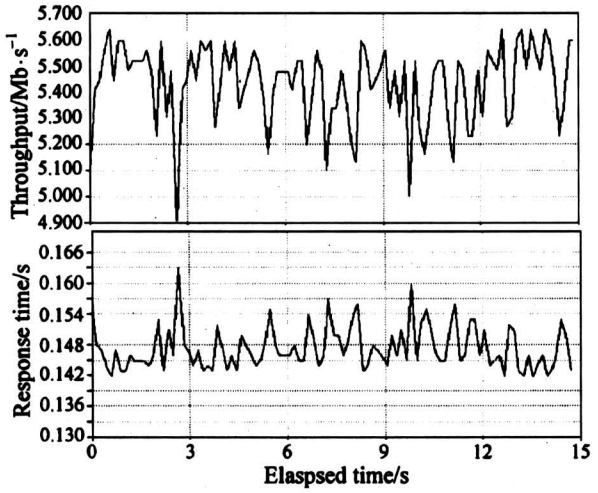

图 4　无线接入点性能测试结果

Fig.4　Performance test of access point

5　结语

系统地分析了 Linux 网络设备驱动的结构体系和系统内核 PCMCIA API 接口，结合实际项目并利用目前国际上最新的和最流行的主流测试工具，论述了基于嵌入式 Linux 操作系统的无线接入点网络驱动的设计、实现和测试结果。所开发的无线接入点已经通过验收，成功地投入生产，并且运行良好。所介绍的网络驱动软件开发模块、流程和测试

工具对其他设备的网络驱动开发和测试也具有一定的参考价值。

参考文献

[1] 魏永明，骆 刚. Linux 网络驱动程序，第二版[M]. 北京：中国电力出版社，2002

[2] Hinds D. Linux PCMCIA Programmer's Guide [DB/OL]. http://pcmcia-cs.sourceforge.net, 2003-01-22

[3] LMSC of the IEEE Computer Society. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications [S]. IEEE Standard 802.11, 1999

[4] 毛操德，胡希明. Linux 内核源代码情景分析[M]. 杭州：浙江大学出版社，2001

[5] 苗启广，杨思燕. 基于 Linux 的 ATM 网卡驱动程序研究与实现 [J]. 计算机工程，2004，(4)：55～56，177

Design and Developing of the Network Device Driver on Embedded Access Point

Wang Zhili, Hu Aiqun, Song Yubo

(*Research Center of Information Security, Southeast University, Nanjing* 210096, *China*)

[**Abstract**] This paper systematically introduces the main structure of network device driver based on embedded Linux. With the PCMCIA API, the software modules of embedded AP (access point) and the developing course are stressed. The testing results of the network device driver are given at the end of the paper.

[**Key words**] embedded linux; network device driver; PCMCIA

(上接第45页)

[7] 槌田敦(日). 资源物理学 [M]. 朴昌根译. 上海：华东工业学院出版社，1991. 32～36

[8] 汪应洛，刘 旭. 清洁生产 [M]. 北京：机械工业出版社，1998. 39～40

Study on Environmental Effect Under Different Industrial Production Modes Based on Entropy

Chu Hailin, Li Jun

(*School of Economics & Management, Southwest Jiaotong University, Chengdu* 610031, *China*)

[**Abstract**] The impropriety industrial production mode is one of the main causes of environmental pollution. From thermodynamics, this paper analyses the entropy essential of the pollution of industrial production. On the basis of this, a dynamic equilibrium entropy flow model is set up to measure the infection of industrial production to the environment. Taking three production modes for example, the entropy increase quantity is calculated by using the model and the environmental effect trends can be educed. It can provide decision-making basis for choice of sustainable production mode.

[**Key words**] entropy increase; environmental effect; the industrial production mode; sustainable development