一种基于国产翼辉操作系统网络数据透传功能的实现

王尊廷
（中国电子科技集团公司第七研究所，广东 广州 510310）

摘 要：随着国产化需求的日益提升，国产操作系统的发展也是日新月异，翼辉（SylixOS）作为其中一个典型的代表，内核自主化率达到100%（依据工信部评估报告），拥有完全自主可控的技术能力，在工业自动化、军事、通信、民用等领域发挥着至关重要的作用，而在SylixOS下的开发需求也是千变万化，本文针对在国产翼辉操作系统（SylixOS）下网口透传功能的实现进行阐述，主要实现网口链路层数据的抓包、分析，然后根据需求选择进行转发。

关键词：原始套接字；SylixOS；网卡混杂模式；网卡绑定；网口透传
中图分类号：TP393.0　　**文献标识码**：A　　**文章编号**：1004-7344（2021）31-0272-02

0 引言

实现数据透传的两种常见方式：①系统路由配置；②原始套接字编程实现。

系统路由配置是最简单方便的方式，但实际应用中可能会受一些其他因素限制无法使用。原始套接字虽实现较为复杂，但透传数据细节可自行控制，可对数据进行处理或筛选然后进行透传，由于项目中用到无线板卡进行无线数据收发，而无线板卡对转发的数据有一些限制，无法使用路由转发功能实现数据透传，因此本文主要讨论第二种：原始套接字编程实现网络透传功能。

1 透传功能实现

1.1 原始套接字和标准套接字的区别

流式套接字和数据报套接字这两种套接字工作在传输层，主要为应用层的应用程序提供服务，并且在接收和发送时只能操作数据部分，而不能对IP首部或TCP和UDP首部进行操作，通常把这两种套接字称为标准套接字。

如果我们开发的是更底层的应用，比如发送一个自定义的IP包、UDP包、TCP包或ICMP包，捕获所有经过本机网卡的数据包，伪装本机的IP，想要操作IP首部或传输层协议首部等等，这些功能对于这两种套接字就无能为力了。这些功能需要使用另一种套接字来实现，这种套接字叫作原始套接字，功能更强大，更底层。

原始套接字，指在传输层下面使用的套接字，可以读写内核没有处理的IP数据包，可以自动组装数据包（伪装本地IP和本地MAC），可以接收本机网卡上所有的数据帧（数据包）。原始套接字直接置“根”于操作系统网络核心（Network Core），而标准套接字（SOCK_STREAM、SOCK_DGRAM）则“悬浮”于TCP和UDP协议的外围。

1.2 设备组成

无线通信设备组成如图1所示。

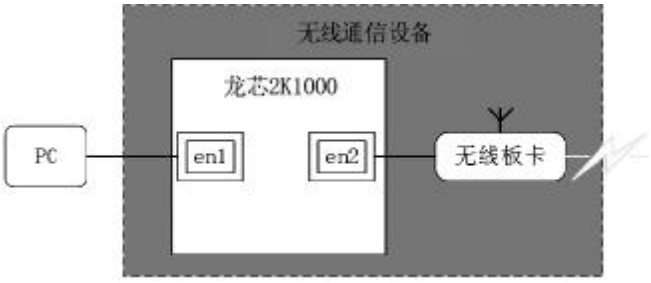

图1 无线通信设备组成

设备采用龙芯最新一代2号处理器2K1000，集成存储、显示、音频、网络等功能，具有高性能，低功耗的特点。操作系统为翼辉信息有限公司开发的SylixOS，SylixOS是一款嵌入式硬实时操作系统，设计思路上借鉴了众多实时操作系统的设计思想，使得具体性能参数上达到或超过了众多实时操作系统的水平，成为国内实时操作系统的最优秀代表之一。

龙芯2K1000网卡en1与用户PC相连，用于接收用户的网络数据，另一网卡en2与无线板卡相连，以便于将网卡en1收到的用户有线网络过来的数据通过网卡en2发送给无线板卡，再由无线板卡发送出去，由另一台设备的无线板卡进行接收，然后通过网卡en2发送给另一台设备的龙芯2K1000处理器，龙芯2K1000再将数据通过en1发送给另一PC，以此实现两个PC之间的数据传输。

对于无线通信而言，空口资源往往很紧张，为了减轻空口数据的压力，经常会对网络数据进行限制。无线网卡为了降低空口资源的压力，只能传输固定源 IP 地址和目的 IP 地址的数据，若要实现两个 PC 之间的数据传输，依靠配置系统的路由转发功能已无法实现，此时可使用原始套接字编程，通过软件编程实现网络数据透传功能。

1.3 透传功能的实现

实现透传功能，需要用到链路层原始套接字，调用 socket() 函数创建链路层原始套接字，第一个参数指定协议族类型为 PF_PACKET，第二个参数 type 设置为 SOCK_RAW，此时接收和发送的数据都是从 MAC 首部开始的，第三个参数是协议类型（该参数只对报文接收有意义），由于不确定 PC 端过来的数据是何种协议的数据，所以此处第三个参数选择 ETH_P_ALL（报收本机收到的所有二层报文）。

设备处理器网卡 en1 使用链路层原始套接字，网卡 en2 使用标准套接字编程，实现两个 PC 之间的数据透传功能。设备处理器中程序需要通过原始套接字在网卡 en1 处抓取数据，对数据进行分析，选取需要透传数据，将数据内容（包含 MAC 头的完整数据帧）作为 UDP 数据包内容，通过标准套接字网卡 en2 发送给无线板卡。无线板卡之间为无线传输，标准套接字在网卡 en2 处读取无线板卡的数据，然后取出 UDP 的 data 部分，通过原始套接字编程的网卡 en1 发出去，设备处理器内部程序处理流图如图 2 所示。

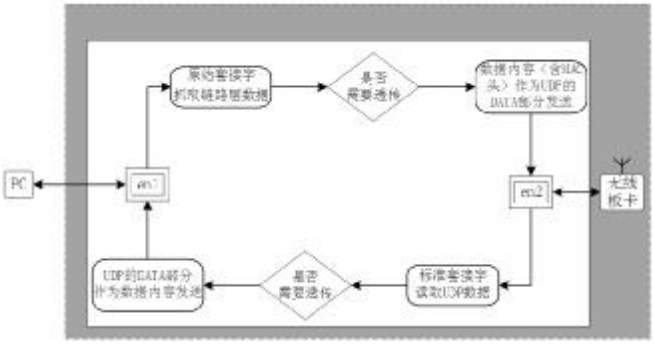

图 2 程序处理流图

两个设备之间程序处理完全一样，唯一不同的地方是在网卡 en2 进行标准套接字编程时，两台设备的源地址和目的地址相反，源端口和目的端口相反。

此时可实现两个 PC 之间的网络数据的透传，由于原始套接字实现的是链路层数据的抓取和发送，因此可实现基于链路层以及上层协议的所有网路数据传输。可透传数据包含 ARP、RARP 以及基于 IP 协议的所有上层数据。

1.4 注意事项

（1）设置网卡为混杂模式，可以抓取到非本机 MAC 地址的数据，此功能可以使用集线器进行测试，网卡设置为混杂模式，程序就不需要进行复杂、频繁的 MAC 地址替换了，可以减少大量的替换工作。Linux 系统设置网卡混杂模式后，可以通过 if-config 查看到混杂模式是否设置成功，但是 SylixOS 系统无法通过此命令查看，可以通过 ioctl 命令查看当前网卡的模式，具体实现如下：

①struct ifreq ifr；

②ifr.ifr_flags|=IFF_PROMISC；

③ret=ioctl（socket_fd，SIOCSIFFLAGS，&ifr）；/* 网卡混杂模式的设置 */

④if((ifr.ifr_flags & 0x400)==0)

⑤ {/* 通过查看 ifr_flags 是否包含 0x400 来确认混杂模式设置是否成功 */

⑥printf("%s net PROMISC set error \n"，Eth_Name)；

⑦}

（2）实现网卡 en1 原始套接字编程时，需要绑定网卡 en1，不然会将所有网卡数据抓取出来，根据抓取数据的网卡，判断数据来源和数据的处理方式。原始套接字不支持 SO_BIND-TODDEVICE 方式绑定网卡，因此需要采用 bind 函数，函数实现如下：

①sll.sll_family=AF_PACKET；

②sll.sll_ifindex=if_nametoindex（Eth_Name）；

③sll.sll_protocol=htons（ETH_P_ALL）；

④bind（socket_fd，（struct sockaddr*）&sll，sizeof（sll））

（3）抓取到数据后，需要根据数据源 MAC 地址判别是否为本网卡发送出去的数据，本网卡发送出去的数据不需要转发，抓取到的其他数据可根据需要对数据进行处理、过滤和转发。

2 结语

原始套接字对于监听网络流量和分析网络数据很有作用，多应用于高级网络编程，也是一种广泛的黑客手段。著名的网络 sniffer（一种基于被动侦听原理的网络分析方式）、拒绝服务攻击（DOS）、IP 欺骗等都可以通过原始套接字实现。

本文只是原始套接字使用的一个实现，两个设备之间通过原始套接字的使用，完成网络数据透传功能，将两个 PC 之间从有线到无线的连接起来，在设备中可对两个 PC 之间的网络数据进行处理和过滤，由于是链路层数据抓取，因此数据包的所有内容均可获取，可根据数据的 MAC 地址、IP 地址、端口号亦或是数据内容等，来决定是否进行数据透传。

设备连接图中的 PC 也可是一个网络，在无线资源允许的情况下，将两个有线网络通过无线的方式连接起来。

参考文献

[1] 北京翼辉信息技术有限公司.SylixOS 应用开发手册[Z].2016.

[2] 宋敬彬，孙海滨.Linux 网络编程[M].北京：清华大学出版社，2010.

收稿日期：2021-07-14

作者简介：王尊廷（1987— ），男，汉族，黑龙江哈尔滨人，本科，助理工程师，主要从事无线通信设备软件研发工作。