pktRxTx使用说明

一、介绍

1. 工具简介

pktRxTx可以监听网卡，收发网络包，支持Windows，Linux，Mac平台。

实现操作网卡时，Windows平台调用WinPcap库，Linux和Mac下调用libpcap库。

使用前，需要安装相应的库。其中，Windows下还需要安装winpcap程序员开发包，即WpdPack。

2. 文件描述

pktRxTx.zip是源文件压缩包。

其中，

Linux/Mac下编译使用**Makefile**编译

Windows下编译是运行批处理脚本**build.bat**

3. 两种模式：

（1）echo模式

echo模式下，收到发往本机的网络包后，修改源和目的MAC地址，然后将包发送回去，即把所有的包都弹回去。

（2）listening模式

该模式只监听接口，不回网络包。同时根据输入控制，即收到一个命令发几个包，然后继续解析下一个命令。

Linux下 以listening模式运行时如图：

```
[wenqing@infgen pktRxTx]$ sudo ./pktRxTx -m 2
[sudo] password for wenqing:
pktRxTx: build at Nov  1 2018, 21:17:02
1. enp1s0f0 (No description available)
2. enp2s0f0 (No description available)
3. lo (No description available)
4. Pseudo-device that captures on all interfaces
5. Bluetooth Linux Monitor
6. Linux netfilter log (NFLOG) interface
7. Linux netfilter queue (NFQUEUE) interface
8. D-Bus system bus
9. D-Bus session bus
10. enp2s0f2 (No description available)
11. enp2s0f3 (No description available)
12. enp3s0f0 (No description available)
13. enp1s0f1 (No description available)
14. enp2s0f1 (No description available)
15. enp3s0f1 (No description available)
Enter the interface number (1-15):2
90:e2:ba:15:cd:d0 ... listening on enp2s0f0
send packets to 10:1b:54:84:83:d6

Input command('quit' for exit)
For example, 'send 5' for sending 5 packets.
> send 4
> send 5
>
```

二、使用

目前，为了跨平台方便，程序中的MAC地址是固定的，所以需要根据运行环境，手动修改pktRxTx.c 中的源和目的MAC地址，如：

```
68 /* fixed MAC address for now */
69 unsigned char src_mac_addr[6] = { 0x00, 0x0e, 0xc6, 0xd7, 0x77, 0x7b };
70 unsigned char dest_mac_addr[6] = { 0x80, 0xfa, 0x5b, 0x33, 0x56, 0xef };
```

1. Linux/Mac

$ cd pktRxTx/

$ make

$ sudo ./pktRxTx -m 1

（注意，调用libpcap获取网卡设备的信息需要root权限，所以Linux和Mac下运

行时需要sudo或直接以root运行）

2. Windows

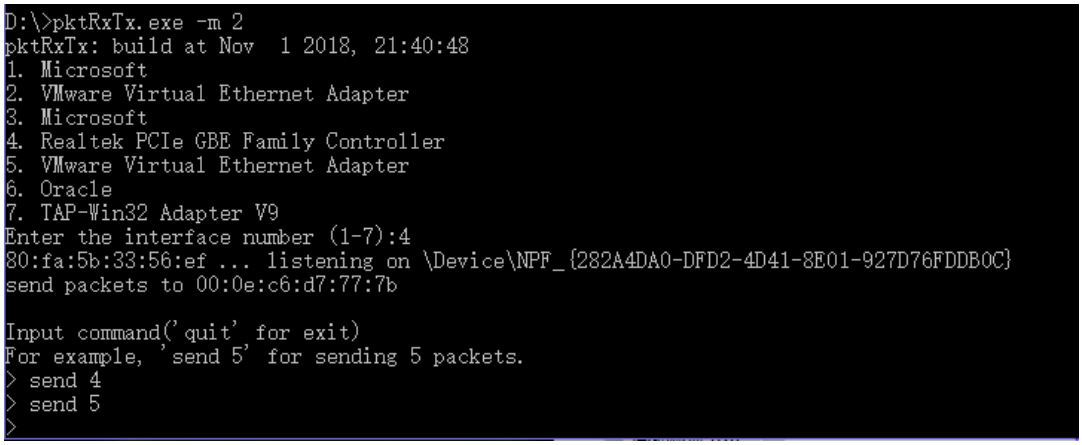
打开命令提示符，进入pktRxTx.exe所在目录

> build.bat

> pktRxTx.exe -m 2

（注意：根据WpdPack目录修改build.bat（或者直接将WpdPack的Include和lib加到系统环境变量里面））

如图，



注意，

- 若Windows机器上缺少库文件，可能报“缺少XX.dll文件”，可以通过安装Visual Studio来安装必要的库文件

3. 命令行选项

-h：

打印help信息；

-m 运行模式：

1， echo模式，即反弹所有网络包；

2， listening模式，可以接收命令，发送指定数量的网络包；

如： -m 1

-i 网卡：

指定监听和发包的网卡，若未指定，程序会打印网卡列表，供用户选择；

如：-i eth0

例如，Mac下以echo模式运行，监听网卡en10，命令为：

```
$  sudo ./pktRxTx -m 1 -i en10
```