开源开发库:libpcap

解码程序依赖库:

1. libxml2, libxml2-devel
2. libpcap
3. gcc 编译环境

目前tcpFlowParse只支持银联前置.

# 一.解码程序安装:

解码程序tcpFlowParse.zip

操作用户必须是root

1.拷贝tcpFlowParse.zip到/opt目录下,解压缩

unzip tcpFlowParse.zip

2.进入 tcpFlowParse目录

cd tcpFlowParse

3.清除历史编译

make clean

4.编译当前系统的程序

make

# 二.配置解码程序

配置文件目录在/opt/tcpFlowParse/etc目录下

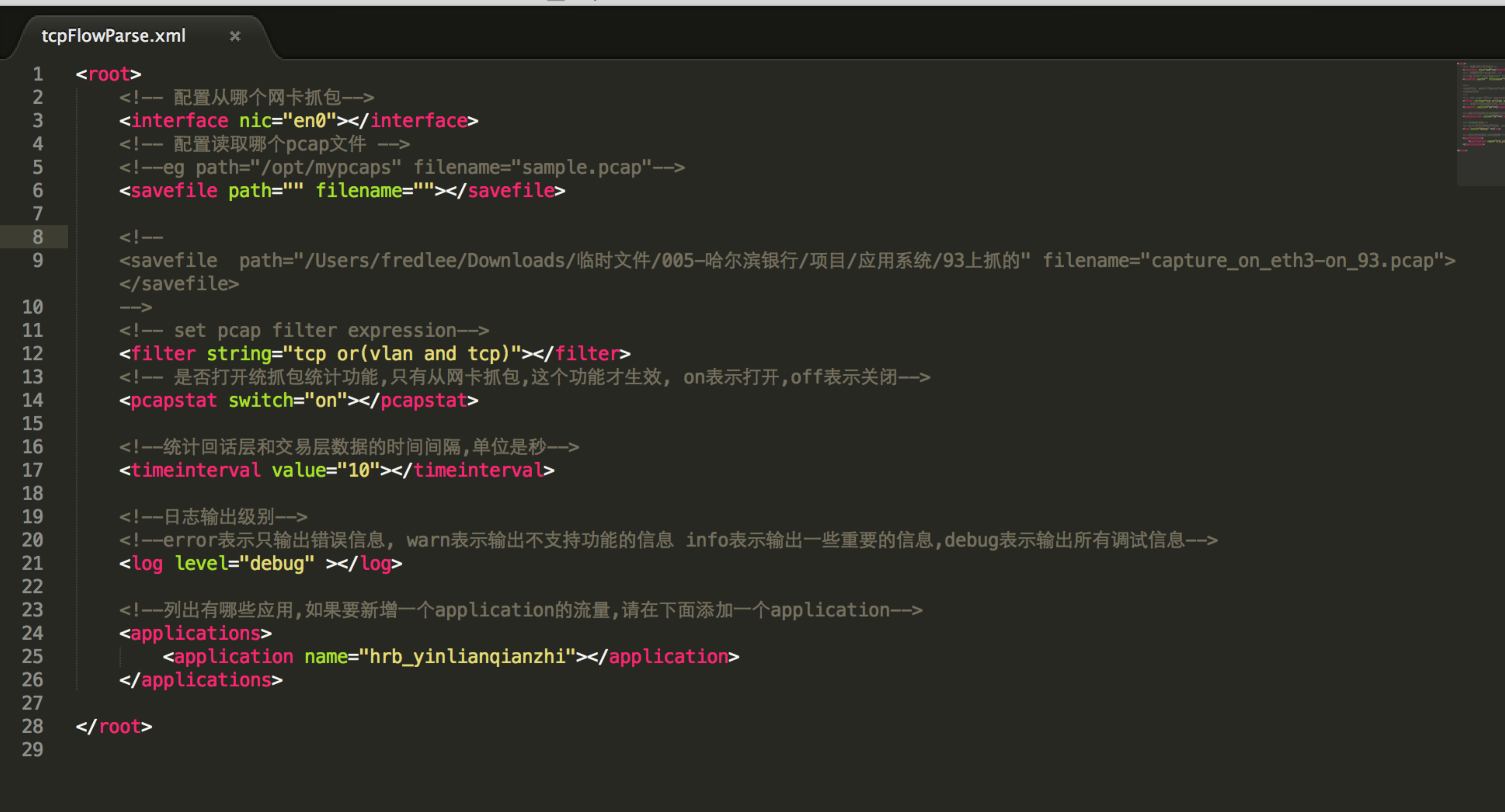
tcpFlowParse.xml 保存整个程序配置信息

applications目录 保存银联应用系统的相关系统

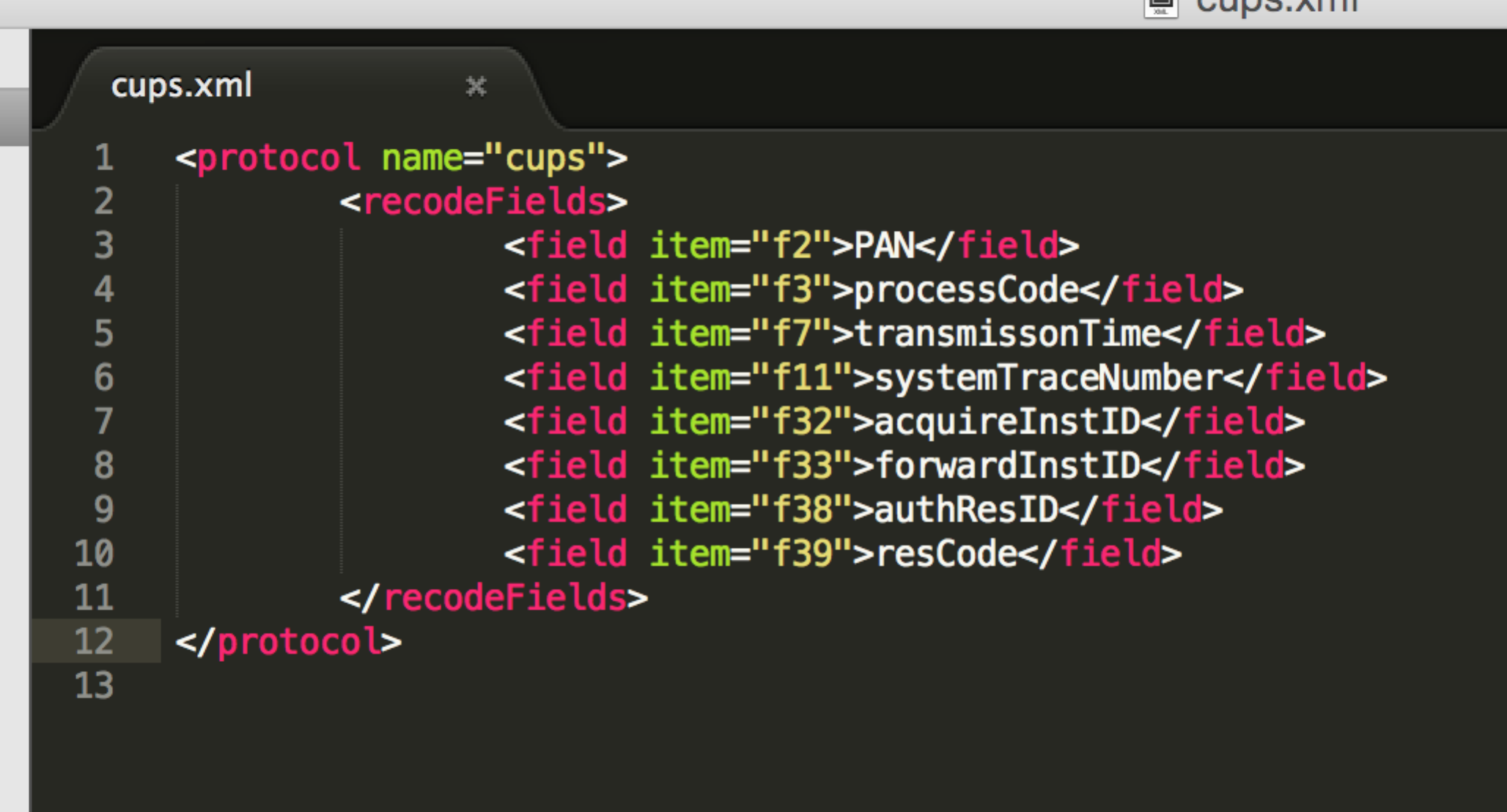
protocols目录 保存银联数据协议的信息

其中tcpFlowParse.xml

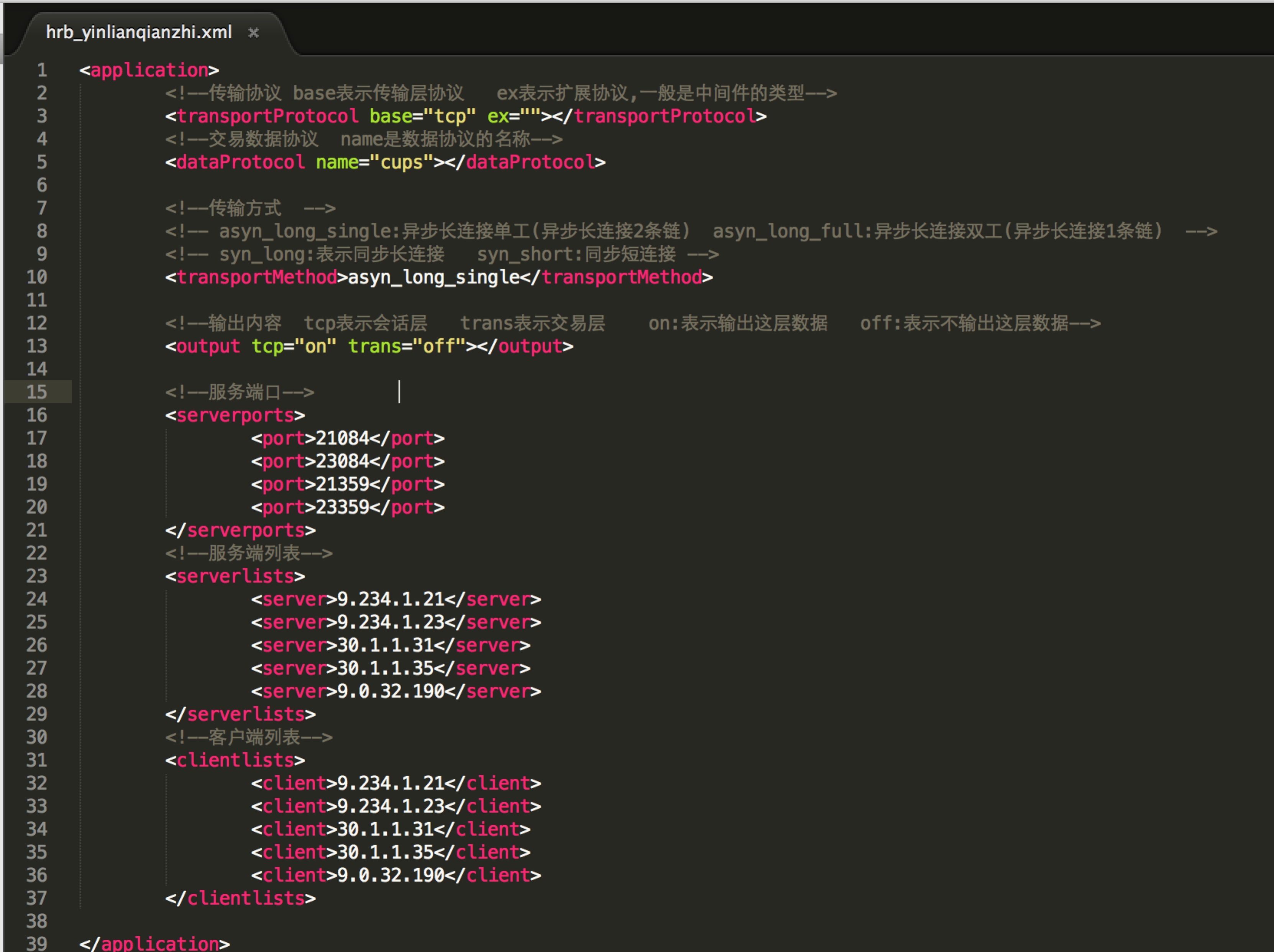
主要配置从哪个网卡抓包,其他的默认即可



其中protocols/cups.xml保存银联cups协议字段信息



其中applications/hrb\_yinlianqianzhi.xml保存银联前置的ip,端口信息



# 三.程序的启停

程序安装在/opt目录下

进入/opt/tcpFlowParse/bin目录下

启动程序:

./tcpFlowParse

停止程序:

./tcpFlowParse -s stop

程序启动后,在/opt/tcpFlowParse目录下会生成两个日志文件

\*.log 保存程序运行日志

\*pid 保存程序pid

# 四.分析交易日志

在/opt/tcpFlowParse/var目录下有交易日志

其中目录是交易系统的名称,进入目录会有分析的交易日志

# 五.后期维护

有两种方式:

方式一:

提供新的tcpFlowParse.zip包

1)停止原来的tcpFlowParse程序

./tcpFlowParse -s stop

2)把原来的tcpFlowParse目录移动到/tmp下,或者直接删除掉原来的tcpFlowParse目录

3)解压新的tcpFlowParse.zip到/opt下

4)编译,配置,启动新的tcpFlowParse

方式二:

直接使用rpm -ivh 安装

安装后在配置,启动tcpFlowParse.

# 六.分析流量包思路

