一、故障现象

Modem放置三四天后，提示连线跟踪的缓冲区已经满了，此时LAN口ping modem无法ping通，网页无法访问。

故障整了两三个星期解决，但有很多感触。

二、故障分析

初步分析，是nf_conntrack_count这个计数只增长不下降，导致连线一直被占用。

打印/proc/sys/net/netfilter/nf_conntrack_count，发现连线记录一直在增长不减少。

打印nf_conntrack的hash表和safe_list这两个表，发现导致出错的包是SSDP包。**也就是说包被释放掉了，但是连线没有删除。**

这个时候去追溯nf的释放过程。skb被free掉了，但是连线记录还在被占用。

在bcmxtmrt.c的发包函数中加打印，发现SSDP包并没有从WAN口发送出去。

在wb_device.c的发包函数中加打印，发现SSDP包有进入这些函数，但是没有从这些函数出来。定位到出错的位置。

wb_device.c的发包函数会对组播包作特殊处理，且有用户态代码配合，我们没有这些代码导致出错。

三、总结

1. 故障现象的收集

（1）故障加速复现。通过修改nf_conntrack_max，故障很快都能复现出来。但是，没有更进一步地找到故障的复现规律。包括以下：

· 插上DSL线后，故障才能够出现。也就是说，复现条件之一是有WAN接口。

· 与WAN接口有关系，也就是与具体的业务可能有关系。IGMP Snooping配置开一下后，就会出现故障。但是后来通过看代码，知道配Snooping后，会重新配置所有WAN连接，所以没有关系。

· nf_conntrack的连线计数net->ct.count，可以通过/proc/sys/net/netfilter/nf_conntrack_count读取，当这个计数一直增长时，就可以认为故障出现了。更加地准确。

· SSDP是组播包，组播包会发往所有的接口，但是抓去镜像以及LAN口，只有LAN口的收包。

· 打印内核中记录的连线，可以确定丢的是什么包。

2. 添加打印

· 全面，比如在打印连线信息时，先只打印源IP，又只打印源IP、目的IP，最后才把信息打印全面(srcIP、destIP、ct->count等)。更进一步，只打印hash表，却不打印safe_list。

· 有效，确定无意义的打印，要及时去除。以免干扰。

· 执着，找到一个出问题的原因，就要一直查下去。比如在打印hash表的那个下午，不停受到打断，最后自己都没有把这个列表完整打印出来分析。

3. 写代码要全面

· 释放包的时候，要参照其他的代码写标准的流程，而不是直接调用skb_free(skb)。

· 条件语句时，或者有#if宏的时候，各种代码分支都要考虑到。容易遗漏#if宏。

4. 连线跟踪计数一直在增加，但是此时业务却是正常的。那么肯定是因为某种错误，包被释放了但是连线没有释放。此时可以打印连线跟踪的所有条目，也可以根据包的流程。比如在PPP、WB、XTM各层打开包打印开关，分析有哪些包在往外发。

在分析该故障时，一直没有这种思路，浪费了很多时间。