## 问题：

反复进行/etc/init.d/network reload命令，出现内存泄漏。

## 现象：

1、使用free查看，可用内存逐渐减少，并且通过echo 3 > /proc/sys/vm/drop\_caches无法进行回收。

2、使用ps、top查看，内存未被应用层占用。查看内核内存，SUnreclaim逐渐增多，此处表示不可回收slab内存。

3、查看slabinfo信息，占用内存主要集中在kmalloc-4096 与skbuff\_head\_cache上。

## 调试与分析记录：

### 11-23

1、根据全海邮件，查验ntp是否对内存有影响，实验结果来看，为看出变化。

### 11-24

1. 使用wifi reload和wifi reload\_legacy进行测试，内存会持续性减少，被占用的内存同样集中在kmalloc-4096与skbuff\_head\_cache上。
2. 范围从network缩小集中到wifi上。

### 11-25

1. 每次操作都将wifi模块重新加载，卸载wifi模块，仍然不能将增长的内存释放，这样让我怀疑，要么就是在泄漏， 要么便是被内核占用。
2. Wifi不变启动进行配置，范围进一步缩小。

### 11-27

1、全海反馈仅仅使用wifi reload，他那边没有出现内存占用问题，因此我只有使用原始版本和demo板来测试该问题。

2、demo板同样会出现内存增加被占用的问题。

### 12-1

1、仅仅只做加载或卸载无线模块，便可以复现出内存增加被占用的问题。

2、仅仅只做加载或卸载qca\_ol模块，便可以复现出内存增加被占用的问题。这时候无线接口并没有创建，因此跟hostpad与wifi配置可能无关，只与qca\_ol模块加载是占用的内存有关。

3、范围基本缩小到芯片初始化流程。

### 12-2

1、经过跟全海交流，他们也查到了在初始化无线芯片的时候，发生了内存泄漏。

2、case已经提到了高通RD。

### 12-5

1、分析芯片初始化，基本确定与BMI阶段有关。

2、ol\_target\_init阶段分析函数ol\_transfer\_bin\_file，传输文件到wifi芯片中，会涉及到dma地址，描述符等底层传输信息。

3、ol\_transfer\_bin\_file使用到vmalloc来分配bin文件所需空间；也是用高通封装的amem（底层使用kmalloc）分配内存，用于传输到wifi芯片。

4、ol\_transfer\_bin\_file最后均对这些内存做了释放，应该不存在内存泄漏。

5、ol\_target\_init阶段分析函数hif\_exchange\_bmi\_msg，交换bmi信息，会涉及到dma地址，描述符等底层传输信息。

6、hif\_exchange\_bmi\_msg中会使用qdf\_mem\_malloc来分配内容，但最后都有释放。

7、hif\_exchange\_bmi\_msg最后调用ce\_send，向ce发送内容。

### 12-7

1、合入memleak补丁，经过测试，kmalloc-4096与skbuff\_head\_cache已无增加趋势。

2、观察补丁的代码，是因为HTC向target发消息，同样通过类似skb包来进行配置，内存泄漏点在skb中数据buff没有得到释放，只释放了skb导致。

3、ol\_target\_init\_complete阶段会做wmi初始化（htc\_wmi\_init）、配置htc与target之间消息管道。

4、htt\_attach\_target函数中，htt向target发送配置消息，配置消息skb的数据buff发生了泄漏。

5、WMI是控制通道，连接host与target。HTT是数据通道，连接host与target。BMI是BootLoader message interface，启动信息通道。

6、BMI中，发送时ce0与收是ce1；WMI/HTC中，控制数据，发送时ce2与收是ce3；WMI/HTC中，管理数据与无线真实数据，发送时ce4与收是ce5；

## 解决方案：

1、将泄露的内存统一放在freelist中，但进行dettach操作时，统一释放。