这是一个耗时很长时间的故障。
为什么这个故障解决了一段时间之后，仍然有malloc出错的问题。

单板启动后，分配一个page的内存，从内核态尝试读取死机文件是否存在。如果存在，则将死机文件写入到/data/die文件下，并清空死机文件的内核page。
首先，用户态只分配一个page的内存，但是在内核态往用户态拷贝内存的时候，却有可能超过一个page。
另外，清空死机文件的page时，内核态只有一个page来存放死机文件的信息，但是却有可能清空超过一个page。
这一起，都是因为strlen的长度不受控导致。
再往前追溯，发现死机文件生成的时候，没有考虑buffer的长度，导致有可能写的时候就发生越界。那么，有可能在第一次出现异常的时候，因为写越界，出现再次异常。也有可能第一次异常之后，单板自动重启，由于只预留了一个page，所以该page之后的那个page被分配出去，但是由于当前page没有'\0'结束符，导致在用strlen的时候，memset将这个page之后的一段内存给清空掉，且被清空的内存的范围是不可预料的。因为这之后的page的内容是vmalloc分配的，有可能是代码段，也有可能是数据段。

---

1. 异常映射表如何查看？
2. 无线模块的地址映射。比如死机文件越界，越到什么地方去了。
3. 什么是DMA重填。
4. 加速复现的方法。
5. 如何将一块内存设置为写保护。

陆亦芬的故障分析

8月02日 计划及进展：

初步分析了下保存日志的函数，发现没有作长度校验，即可能会出现保存的日志长度超过预留的内存区间，从而破坏其他内存区间中的内容。继续测试，发现出现问题的时候，保存的日志长度已经超过预留的内存区间了，即越界了，这应该是引发这个故障的原因，也符合理论分析。

修改日志保存的代码，在保存时，校验长度，如果长度超过预留的内存空间，则不再继续保存日志，使用以前复现的方法，复现了10次，都没有出现问题，今天继续拷机，如果到明天早上还没有出现，则这个问题应该已经解决了，

8月01日 计划及进展：

初步分析了下无线的中断处理函数，没有发现明显的问题。

经过几天的实验能够想到的也基本都做了，目前也没什么好的办法，今天打算看下H168N与H368N相关代码差异，重点看下配置相关部分以及我们怀疑的内存管理相关的代码。

1. 发现配置文件中有一些差异，但分析认为应该不可能导致异常，实验证明这个差异对故障不产生影响。
2. 发现在H168N中有一个关于保存异常日志的代码，分析认为这应该是一个疑点，明天继续实验验证。

7月31日 计划及进展

今天主要想对内存破坏区域进行跟踪，看是否可以跟踪出谁对该区域进行操作；

1. 改变无线代码段布局，在加载无线代码段之前使用vmalloc申请一片区域放在那不用，然后再进行无线模块内存申请，无线申请完之后再进行申请一片区域，然后进行复现，很快系统出现了内核异常，而且出现很多次异常，并且异常点不确定，另外读取映射表发现映射地址有0x80000000这样的，按照道理这个地址空间不应该被映射的。
2. 在无线加载时候将代码设置为写保护，主要是想看下谁破坏这个区域，系统会报出异常，但是通过实验发现内核异常到处飞，基本上都乱了，但是并没有看到谁破坏了这个区域。
3. 将无线校准部分代码进行关闭硬中断，看下是否是因为无线执行过程被硬中断打断，通过试验发现关闭中断后系统异常点变了，不在无线校准函数里面，其中一次出现在cpsd里面难道与中断有关系？下一步准备跟踪下中断部分代码。

7月30日 计划及进展

目前主要打算对无线校准部分继续分析，查找无线校准部分执行是否会被其他部分抢占以及是否存在分配内存等相关问题；

1、异常的时候在函数回溯中总会看到无线校准的函数，怀疑是校准被无线的其他处理流程抢占导致，于是在无线校准函数执行时，将抢占关闭，但是仍然会出现问题；

2、通过看无线代码发现里面有DMA重填部分，因此怀疑是否是内存不足时重填DMA失败导致内存被破坏，因此在代码中将DMA重填注释掉，然后进行主动式复现，经过复现，发现该问题仍然会出现。

7月28日计划及进展：

1. 主要怀疑无线校准函数部分导致代码段被破坏，因此打算对无线校准函数进行跟踪。
2. 由于无线校准函数很复杂，且涉及很多底层的寄存器，而寄存器又没有给我们开放，因此大家对代码都不熟悉，所以只能采取最简单的方法来简化无线校准函数的处理流程，然后进行反复的主动式复现，但是经过大量复现后发现这种做法并不可靠，由于该函数比较复杂不宜跟踪，另外在某些点复现3次以上后并不能100%保证此点就一定没有问题，如果复现次数太多的话时间上会太长，因此暂时放弃了这种做法。

7月27日计划及进展：

1、排除内存不稳定的猜想，现在主要怀疑内存映射表被破坏，或者存放代码段的内存直接被破坏，需要继续验证；

2、在die函数里面增加代码将EPC附近的值及内存其他部分打印出来，通过复现异常时候发现EPC

附近无线代码段的值被破坏了，而内存其他部分的内存是正确的，因此内存不稳定的猜想基本排除了；

3、对页表映射项进行验证，主要将单板起来无线虚拟地址空间部分内容打印出来，然后在出现内核异常时候将其内容与之前相比较发现，除部分被破坏除外其他内容相同，因此可以基本确定映射表项是正确的；

上面几个猜想基本上都否定了，下一步打算跟踪下无线校准部分函数，因为异常点每次都出现在无线校准部分函数。

7月26日计划及进展：

1. 由于之前的复现方法比较慢，因此打算采用主动式复现的方法进行复现，主要考虑将内存耗到临界的情况，然后再进行通过跑大流量业务，由于实验室无线环境比较复杂，很难跑起来，基本上断断续续，因此将有线流量加大，采用Iperf发送50M流量进行拉流量增加系统负载；
2. 通过验证发现在大流量情况下，使用测试程序，将系统内存消耗到临界状态后再进行跑业务，到今天上午10点半左右，已有三次在耗尽内存时，出现reserve指令的问题，目前正在摸索规律，希望可以快速必现；
3. 分析异常日志，以及适时增加调试代码，以确认究竟是内存不稳定还是内存中的内容被代码异常破坏导致。
4. 通过反复的主动式复现，寻找故障出现规律，基本上能够做到将故障在二十分钟内必现；

7月25日计划及进展：

1. 上午将增大实验室拷机环境中的流量，并在拷机过程中增加一些操作。如果上午仍然无法复现，则下午考虑去翠岛拷机复现，需要协调翠岛的环境；
2. 由于在前面的日志中，看到内存不足后，无线驱动中会出现reserve指令的异常，但从理论分析，即使内存不足，也不应该出现reserve指令的问题，所以打算写一个小的APP，把内存基本耗光，看是否可以复现故障。
3. 由于环境原因，先在小流量情况下，使用测试程序，耗尽系统内存，只出现了内存不足的情况，并没有出现reserve指令的问题；
4. 在实验室的拷机环境中，增大拷机流量后，出现了两次单板挂死现象，挂死后系统无任何响应，这在以前的拷机中并没有出现过，在第一次出现挂死后，在版本增加调试代码，记录系统挂死时执行的指令地址，第二次出现系统挂死后，检查发现挂死点在系统的异常向量表中，这可能是由于内存中异常向量表被破坏导致；
5. 出现了一次reserve指令的问题，与之前的故障现象基本一致，分析发现可能从内存中所读的内容不正确导致，理论分析，这可能是内存不稳定或者内存中的内容被破坏导致，于是，根据我们的猜想加入了相应的调试代码，在出现问题的时候，把异常地址对应的内容，以及其他地址中的内容打出来，继续拷机。

实验室的无线环境并不稳定，请求了其他相关同事的支援，所以在搭建无线环境上也花费了一定的时间。

7月24日进展：

1、在实验室搭建好拷机环境，主要业务：

有线侧的视频IPTV，ftp下载,PING大包65000，

无线侧的ftp下载，PING大包65000;

2、搭建好版本编译环境，版本已经编译好；

3、对武研所提供的日志进行了分析，对故障有了进一步的了解。

陈强到南京的出差报告

7.20

下午到南京后，与吴二刚等人来到测试地点，搭建环境，单板为测试部单板，业务为两台PPS，4台下载BT，在重新更换配置后，系统刚上电一会，发生了一次epc，并重启，其epc为epc ：c063effc wlc_phy_radio205x_check_vco_cal_nphy+0x28/0xfc [wl]。 该地点与测试部先前发给log类似，也是在wlc_phy_radio205x_check_vco_cal_nphy函数里面写寄存器的地方。发回后方分析，仍和以前一样无法看出什么。

后尝试继续尝试复现到8点，仍未能复现，故搭建拷机环境拷机。

7.21

早上来后发现，电视仍在继续播放，没有重启发生。看log也没有epc产生。故友重新调整bt，重新开始等，pps换台，仍没有挂死发生。
下午换刘金成带来的单板重新测试，业务不变。一下午尝试各种操作，包括迅雷连接中断，pps换台，电视直播和点播等。单板仍无挂死的现象。
晚上，添加脚本，通过按键精灵，不断反复的on/off RF，拷机。

7.22

早上，发现昨天wlan反复切换的脚本，仍没有epc出现。后来察看各个版本的迅雷信息，包括版本号，配置等，其间单板挂死打印如下：006e26fc (epc == 2af2ad08, ra == 2af2aa24)

do_page_fault() #2: sending SIGSEGV to cspd for invalid read access from

006e26fc (epc == 2af2ace0, ra == 2af2a93c)

18:44:38 [U_pc][Emerg] [pc.c(926)ScanProgram] Process exception:[cspd] pid[308] is in exception

18:44:38 [U_pc][Emerg] [pc.c(2247)InitReboot] Process exception:pc found exception:the system is begining to restart

Found userspace die error, prepare to save.....

Starting pid 25589, console /dev/ttyS0: '/bin/umount'

umount: tmpfs busy - remounted read-only

dst cache overflow

18:44:41 [OSS_cspd][Error] [oss_comm.c(1136)SocketCreate] socket (/var/tmp/0X00000102) in using

18:44:41 [OSS_cspd][Error] [oss_sche.c(490)InitPCBPool] Socket_Create failed

18:44:41 [OSS_cspd][Error] [oss_sche.c(255)OSSStart] InitPCBPool ERROR !!!

18:44:42 [U_pc][Emerg] [pc.c(926)ScanProgram] Process exception:[cspd] pid[25594] is in exception

18:44:42 [U_pc][Emerg] [pc.c(2247)InitReboot] Process exception:pc found exception:the system is begining to restart

The system is going down NOW !!

dst cache overflow

Sending SIGTERM to all processes.

18:44:45 [OSS_cspd][Error] [oss_comm.c(1136)SocketCreate] socket (/var/tmp/0X00000102) in using

18:44:45 [OSS_cspd][Error] [oss_sche.c(490)InitPCBPool] Socket_Create failed

18:44:45 [OSS_cspd][Error] [oss_sche.c(255)OSSStart] InitPCBPool ERROR !!!

18:44:46 [U_pc][Emerg] [pc.c(926)ScanProgram] Process exception:[cspd] pid[25614] is in exception

18:44:46 [U_pc][Emerg] [pc.c(2247)InitReboot] Process exception:pc found exception:the system is begining to restart

igdnat: No such file or directory

PID Uid VmSize Stat Command

发给刘振华分析，无结果，是一个while循环，不太可能挂死。将所有的配置，包括迅雷的种子文件发回所内，所内测试复现了一次挂死现象。

下午，更换版本使用刘振华的memwatch的调试版本，进行测试。采用如下方法测试: 拔掉DSL接口，重启单板，等无线连接后再插上DSL线，第二次测试时，发生重启和20号的类似，挂死的地方为epc ：c0642ff0 wlc_phy_rfctrl_override_1tomany_nphy+0x164/0x364 [wl]，
发给邵存金分析，无结论。

晚上，采用memwatch脚本拷机，使用脚本，每隔5分钟重启一次单板。

7.23

早上，检查昨晚拷机结果，发现多个epc，发给所内分析，证实除了一个epc外，其他的epc打印均是正常的。 有问题的epc为epc ：c05d72c8 si_deviceremoved+0x8/0x54 [wl]， 发给所内分析，是无线ioctl。

下午，继续尝试复现故障，进行各种操作仍无法复现。尝试邵存金发的一个脚本，先down wlan， rm wl.ko后再重启， 故障没有复现。

晚上，更换刘金成发的最新版本库版本，更换为测试部的单板，重新配置，采用reboot脚步拷机。

7.24 早上来检查，没有发生挂死重启现象，单板正常无epc。Pps正在播放。

注：所有业务相同，除跑重启脚本无法开启IPTV外，其他的业务均为2台电脑pps，4台下载bt，2IPTV。

总结：1、故障能复现，但每次出现的位置都不一样，采用了所内提供的所有版本和测试方法，仍未能找到故障位置。

2、比较多的出现在wifi的phy模块，分析看都是挂死在wlan的写phy寄存器的地方。此外还有几次epc出现在其他的地方。

3、故障出现的间隔时间较长，平均一整天才能出现一次。