匈牙利版本按照开发报告进行升级发生flash错误并不断重启故障查证记录

【作者】　　刘振华

【时间】　　20120920

【概述】　H168N新生产的一批单板10块，提交匈牙利版本的系统测试，升级匈牙利版本后，10块单板中有一块出现升级版本后不停的重启。Log如下：

测试给的log如下：

1　故障描述

1. H168N_HU匈牙利版本，基于CSP平台，613001603199，【H168N V1.1.0_HUT1】匈牙利版本按照开发报告进行升级发生flash错误并不断重启。
2. 测试刘涛描述如下：

刘金成和刘振华故障确认：

故障出现后，将单板的打印级别调试为debug，对单板异常时的log进行分析，有两个怀疑点：

1. 可能是版本代码的问题，可先走查log分析一下，故障时wlan_config无线模块在进行无线配置，然后打印的故障二级进程也为wlan_config模块

1192:58:23 [wlan_config][Debug] [wlan_adapter_br(1466)wl_getVer] ____cmd=wlctl ver > /var/wlver_____

eth2 Link UP 100 mbps full duplex

1192:58:23 [wlan_config][Debug] [wlan_adapter_br(1468)wl_getVer] wlctl ver > /var/wlver

wlctl: wl driver adapter not founImemhdr[2]=0x100CE000, pAdslLMem[2]=0x100CE000

d

pSdramPHY=0xA3FFFFF8, 0x80D5D4F 0xDEADBEEF

*** XfaceOffset: 0x5FF90 => 0x5FF90 ***

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

00000008 (epc == 2af2bf74, ra == 2af27758)

*** PhySdramSize got adjusted: 0xD19E0 => 0x1080A0 ***

AdslCoreSharedMemInit: shareMemAvailable=171840

AdslCoreHwReset: pLocSbSta=82718000 bkupThreshold=3072

AdslCoreHwReset: AdslOemDataAddr = 0xA3F9304C

dgasp: kerSysRegisterDyingGaspHandler: dsl0 registered

1192:58:23 [OSS_cspd][Error] [oss_fault_trap.(243)SigHandler] Process <312> receive signal 11, epc == 2af2bf74, ra == 2af27758

1192:58:23 [OSS_cspd][Error] [oss_fault_trap.(245)SigHandler] Signal information:

……

2. 怀疑是flash的坏块导致，分析发现版本升级的时候，nandflash有异常打印

The signiture of version file matches current CPE's signiture!

jffs2_scan_eraseblock(): Magic bitmask 0x1985 not found at 0x00f40000: 0xcac2 instead

jffs2_scan_eraseblock(): Magic bitmask 0x1985 not found at 0x00f40008: 0x0006 instead

stopping CPU 1

……

2　查证过程

日期（20120920）

故障思路：先排除怀疑点1的情况，反汇编libc库，查看异常点epc

分析如下：

将libc库反汇编后，发现epc的点为strlen，且返回值为vsscanf函数，走查故障时的log

发现无线模块在读取无线的版本号时异常。Log如下：

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

00000008 (epc == 2af2bf74, ra == 2af27758)

1192:58:20 [OSS_cspd][Error] [oss_fault_trap.(243)SigHandler] Process <311> receive signal 11, epc == 2af2bf74, ra == 2af27758

1192:58:24 [OSS_cspd][Error] [oss_sche.c(1415)OSS_ExcpShowInf] sfs_config 1103 2 0000 311 4 0/ 3/ 16 150

1192:58:24 [OSS_cspd][Error] [oss_sche.c(1415)OSS_ExcpShowInf] usb_stor A455 3 0000 311 4 0/ 3/ 16 150

1192:58:24 [OSS_cspd][Error] [oss_sche.c(1415)OSS_ExcpShowInf] wlan_config A204 3 0001 311 4 0/ 3/ 16 150

1192:58:22 [OSS_cspd][Error] [oss_fault_trap.(169)ShowStack] 2aefe000-2af56000 r-xp 00000000 1f:00 1071 /lib/libc.so.0

利用H168N的libc反汇编的，异常点epc的值为strlen,而ra为vsscaf

从wlan_config的流程跟踪的话 出现在无线的**wl_getVer**函数中去获取版本信息，在串口下cat /var/wlver文件，读不到，怀疑可能是读到的版本号为空，或者过长，导致字符操作的时候异常。

由于对无线模块不是很熟悉，交由邵存金继续跟踪。

日期（20120921）

邵存金跟踪log及怀疑点，在无线模块中加打印，发现wlver文件为空，并没有值

修改代码后发现，wl.ko模块执行命令失败，lsmod发现无线模块没有加载，手动加载wl.ko模块同样加载不成功，记录如下：

加打印跟踪了该问题，异常原因是由于无线模块加载不成功，**导致wl_getVer**函数执行wl ver >/var/wlver命令时，该文件为空，导致后面读文件做文件指针偏移时出现异常。

Using /lib/modules/2.6.30/extra/wl.ko

insmod: cannot insert `/lib/modules/2.6.30/extra/wl.ko': Unknown symbol in module (8): No such file or directory

注释掉函数wl_getVer中的文件操作，让单板启动起来，查看了下是否有wl.ko文件在文件系统中是存在的,

和华仔讨论了下，同批升级的其他单板都没有问题，就这块板子有问题，怀疑跟flash有关。

另外用同样的板子升级ttnet版本，无线模块也加载不成功。

怀疑与flash有关系，准备分析一下是否由flash坏块导致，也就是怀疑点2

日期（20120924）

从log分析，可能与先前南京发现的brcm的一个故障有关，从log看在boot下和版本下对坏块的判断不一致

flash_read_buf blk 552 error

flash_read_buf blk 553 error

begin image synchronization...

Flashing root file system at 0xb8020000: .....

Error erasing flash block, blk=15

Error erasing flash block, blk=106

Error erasing flash block, blk=407

。。。。。。。

brcmnand_default_bbt: bbt_td = bbt_main_descr

Bad block table Bbt0 found at page 0000ffc0, version 0x01 for chip on CS0

Bad block table 1tbB found at page 0000ff80, version 0x01 for chip on CS0

nand_read_bbt: Bad block at 0x001e0000 15

nand_read_bbt: Bad block at 0x00200000 16

nand_read_bbt: Bad block at 0x00d40000 106

nand_read_bbt: Bad block at 0x00d60000 107

nand_read_bbt: Bad block at 0x032e0000 407

nand_read_bbt: Bad block at 0x03300000 408

nand_read_bbt: Bad block at 0x04500000 552

nand_read_bbt: Bad block at 0x04520000 553

nand_read_bbt: Bad block at 0x05620000

nand_read_bbt: Bad block at 0x05640000

nand_read_bbt: Bad block at 0x06880000

nand_read_bbt: Bad block at 0x068a0000

因此设置烧片器为hardcopy模式，且设置Size of UBA blocks为0x400，将坏单板里边的版本读出来，直接烧写到一个新的flash上，故障复现

而将读出来的版本的后1M区的bbt表填充为FF后，再烧入新的flash，版本能够重新正常启动

因此确认与先前的故障一样，

故障单为：613001516777_荆小刚_20120814_合入broadcom patch：解决boot下和版本下对oob坏块判断的一致性

日期（ xxxx-xx-xx，最后一天 ）

故障的根本原因是由于brcm代码的bug，导致在boot下和版本下对坏块的处理不一致导致。这样版本在启动的时候如果不能正确的识别坏块，会导致版本异常。已同步该故障单

该故障再次出现的主要原因是由于对故障单同步不够及时，在即便最忙的时候，对flash、DSL等底层驱动的同步工作，优先级应该最高，这个是基础工作，如果解决不好，将直接影响版本的稳定性。

3　故障总结

故障现象

　从前方发回来的单板升级版本后，版本不停的重启。

故障分析

分析重启的log，是由于无线模块要从驱动获取版本号信息wl_getver()；但是出现空指针，导致单板strlen异常，首先是这块代码对异常的保护不够。

无线模块没有获得版本号的进一步原因是无线模块加载失败，在版本串口下手动加载同样失败，但是版本中确实有wl.ko的文件。

继续分析升级升级的log发现，版本下认为是flash坏块的地方，在boot下却不认为是坏块。联系到先前南京曾经解决过类似的故障，因此做试验验证是否是同一个故障。

经过将flash的bbt区擦除后升级版本，版本找不到bbt区，然后重建后能正常启动；而如果不擦除的话则不能正常启动的对比测试，基本确定是同样的故障。

解决办法为同步该故障单（613001516777_荆小刚_20120814_合入broadcom patch：解决boot下和版本下对oob坏块判断的一致性 ）

故障根因：故障是brcm代码的固有故障，但是没有及时同步，导致版本发布出现延期。

经验教训：

在故障比较多，且优先级都比较高的情况下，对于小系统的同步单，特别是flash\dsl\eth驱动相关的要及时同步，是第一优先级，因为这些问题虽然是基础问题，但是直接影响版本的稳定性，后果不可估量。

从另一个方面来说，同步已经解决的故障与解一个还未定论的故障相比，同步该故障是最优选择。