

3.0基站产品测试 - 错误 #4407

3.1.3pre1T8版本测试过程中，出现du coredump挂死。

2025-11-10 17:14 - 程 鹏

状态:	进行中	开始日期:	2025-11-10
优先级:	高	计划完成日期:	2025-11-30
指派给:	周 立伟	% 完成:	0%
类别:		预期时间:	0.00 小时
目标版本:		耗时:	0.00 小时
问题归属:	DU	目标解决问题版本:	Rel_3.1.3
发现问题版本:	Rel_3.1.3		
描述			
3.1.3pre1T8版本测试过程中，出现du coredump挂死。 基站长跑91h以上，在计划进行单终端峰值验证时（700M灌包正在灌包），其他三部终端下电，此时出现du coredump。			

历史记录

#1 - 2025-11-18 11:24 - 周 立伟

- 文件 20251118-112324.jpg 已添加
- 状态 从 新建 变更为 进行中

```
[New LWP 1537]
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/aarch64-linux-gnu/libthread_db.so.1".
Core was generated by './gnb_du'.
Program terminated with signal SIGSEGV, Segmentation fault.
#0 0x000000000066760c in cmPrcTmr (tqCp=0x7d5edf4b10, tq=0x7d5edf4b20, func=funcEntry=0x872780 <rgSCHTmrProcTmr(Ptr, OnTimer*)>) at /home/zw/du_push/ran/nr_hl_du/src/cm/cm_bdy5.c:484
484 /home/zw/du_push/ran/nr_hl_du/src/cm/cm_bdy5.c: No such file or directory.
[Current thread is 1 (Thread 0x7fa84cb70 (LWP 1355))]
(gdb) bt
#0 0x000000000066760c in cmPrcTmr (tqCp=0x7d5edf4b10, tq=0x7d5edf4b20, func=funcEntry=0x872780 <rgSCHTmrProcTmr(Ptr, OnTimer*)>) at /home/zw/du_push/ran/nr_hl_du/src/cm/cm_bdy5.c:484
#1 0x00000000000874520 in rgSCHLvl1TomTtiInd (ttiInd=0x64de214 <rgSCHLvl2TomUtlSendStartInd:rgTtiInd+2916>, rgSchLvl1InstCb=0x1207e68 <rgSchLvl1Cb>) at /home/zw/du_push/ran/nr_hl_du/src/5gnrsch/rg_sch_tom_lv1.c:693
#2 0x00000000000875990 in rgSCHLvl1TomProcStartInd (rgSchLvl1InstCb=<optimized out>, startInd=startIndEntry=0x04de3f0 <rgSCHLvl2TomUtlSendStartInd:gsStartInfo+144>) at /home/zw/du_push/ran/nr_hl_du/src/5gnrsch/rg_sch_tom_lv1.c:1186
#3 0x0000000000083f5a0 in RgSchLvl1InfStartInd (schGCh=schGChEntry=0xe39e08 <cmGCh+9768>, startInd=0x64de3f0 <rgSCHLvl2TomUtlSendStartInd:gsStartInfo+144>) at /home/zw/du_push/ran/nr_hl_du/src/5gnrsch/rg_sch_lv1.c:951
#4 0x00000000008277fc in rgSchLvl1ActvTsk (tskInfo=0x7d6cde3030) at /home/zw/du_push/ran/nr_hl_du/src/5gnrsch/rg_sch_cm_hdl.c:121
#5 0x000000000007aa5b0 in gnb_du::gnb_du_worker_thread_instance::process_message (this=0x7d5f229b34, p_task=<optimized out>, priority=<optimized out>) at /home/zw/du_push/ran/nr_hl_du/src/du_app/gnb_mgr/build/./src/gnb_du_worker_thread.cpp:487
#6 0x0000000000074e7c0 in ngp::thread_pool<gnb_du::gnb_du_worker_thread_instance, ssltkInfo>::thread_worker::run (this=0x2ff21480) at /home/zw/du_push/ran/nr_hl_du/src/du_app/gnb_mgr/build/./src/./src/./src/./ngp/include/ngp_thread_pool.h:426
#7 0x000000000008c5b4 in thread_start () at /home/zw/du_push/ngp/thread/build/./src/ngp_sys_thread.cpp:338
#8 0x00000007fbc257e4 in start_thread (arg=0x7fe5216f4f) at pthread_create.c:486
#9 0x00000007fbb8970c in thread_start () at ../sysdeps/unix/sysv/linux/aarch64/clone.S:78
(gdb) f 0
#0 0x000000000066760c in cmPrcTmr (tqCp=0x7d5edf4b10, tq=0x7d5edf4b20, func=funcEntry=0x872780 <rgSCHTmrProcTmr(Ptr, OnTimer*)>) at /home/zw/du_push/ran/nr_hl_du/src/cm/cm_bdy5.c:484
484 /home/zw/du_push/ran/nr_hl_du/src/cm/cm_bdy5.c
(gdb) info locals
bwNormal = <optimized out>
tempTail = <optimized out>
expire = 533733382
entry = 2
entry1 = <optimized out>
tqEnt = 0x7d5edf4b40
tqEnt1 = <optimized out>
cb = <optimized out>
tmpl = <optimized out>
startTime = 0
(gdb) f 1
#1 0x00000000000874520 in rgSCHLvl1TomTtiInd (ttiInd=0x64de214 <rgSCHLvl2TomUtlSendStartInd:rgTtiInd+2916>, rgSchLvl1InstCb=0x1207e68 <rgSchLvl1Cb>) at /home/zw/du_push/ran/nr_hl_du/src/5gnrsch/rg_sch_tom_lv1.c:693
693 /home/zw/du_push/ran/nr_hl_du/src/5gnrsch/rg_sch_tom_lv1.c: No such file or directory.
(gdb) info locals
cellIdx = <optimized out>
nCell = 0 '000'
cell = {0x7d5edf4ac0, 0x0 <repeats 15 times>}
ret = 0
srcsTimeInfo = {hSfn = 0, sfn = 0, slot = 0 '000'}
srcsTimeInfo = {hSfn = 0, sfn = 0, slot = 0 '000'}
ttiIndTick = {0, <optimized out> <repeats 14 times>}
ttiIndDiff = {0, <optimized out>, <optimized out>, 0, 0, 0, 0, 0, <optimized out>, <optimized out>, <optimized out>, <optimized out>, <optimized out>, <optimized out>}
(gdb) █
```

#2 - 2025-11-18 11:28 - 周 立伟

- nCell=0,局部变量内存被踩，怀疑点有3个：
- 1、cell数组越界，踩了局部变量内存；
 - 2、多个U64局部变量使用，rgSCHLvl1TomTtiInd调用栈比较深，存在栈内存溢出问题；
 - 3、cmPrcTmr函数增加了timerList检查处理，会主动修改timerList链表；

#3 - 2025-11-18 11:31 - 周 立伟

- 已针对上述3个怀疑点进行了优化修改，验证中：
- 1、增加cell数组越界保护；
 - 2、将多个U64局部变量变更为全局变量使用；
 - 3、增加cmPrcTmr函数隔离处理（用户面和MAC独立使用各自的cmPrcTmr函数）；

文件

1111.jpg	1.16 MB	2025-11-10	程 鹏
----------	---------	------------	-----

