

```
描述
基站版本：el_2.1.12P_Pre2_Xeon
核心网版本：YZ-Core50000_Rel_3.0.2
终端CPE版本：四信 FNR100V1.1
phy（12pre2）
CU
DU（4月24日）
YZMM：yzmm-V2.1.12P_pre2
其他：5.8GHz环境
问题描述：
1、大上行配置，11终端接入，每个终端上行14M，下行9M流量；
2、长跑3小时左右，出现du挂死退出
堆栈信息如下：
(gdb) bt
#0 0x00000000046897f in cmDynAlloc (regionCb=0xa8fe7d0, size=0x7ffe8c846b1c, flags=0, ptr=0x7ffe8c846b80) at /root/DU/ran/DU_Alpha_Rel/src/cm/cm_mem_wl.c:2542
#1 0x000000000e0d943 in SAlloc (region=1 '\001', size=0x7ffe8c846b1c, flags=0, ptr=0x7ffe8c846b80) at /root/DU/ran/DU_Alpha_Rel/src/mt/ss_mem.c:530
#2 0x000000000e0dff5 in SGetSBuf (region=1 '\001', pool=0 '\000', ptr=0x7ffe8c846b80, size=64) at /root/DU/ran/DU_Alpha_Rel/src/mt/ss_msg.c:1465
#3 0x000000000ad6cba in SPstWTsk (hdr=0x7ffe8c846be0, tsCb=0x7ffe25042020, msg=0x0) at /root/DU/ran/DU_Alpha_Rel/src/du_app/gnb_mgr/build/./src/gnb_du_worker_thread
#4 0x000000000b87120 in kwUtlRcvFrmLi (gUeCb=0x7ffe25042020, datIndInfo=0x7ffe0a708520) at /root/DU/ran/DU_Alpha_Rel/src/5gnrrlc/kw_utl_ul.c:138
#5 0x000000000b251bf in KwLiRguDDatInd (gUeCb=0x7ffe25042020, datInd=0x7ffe0a708520) at /root/DU/ran/DU_Alpha_Rel/src/5gnrrlc/kw_lim.c:110
#6 0x000000000b655a5 in kWUIActvUeTsk (tskInfo=0x7ffe04e58020) at /root/DU/ran/DU_Alpha_Rel/src/5gnrrlc/kw_ul_ue_hdl.c:446
#7 0x000000000ae5447 in gnb_du::gnb_du_ul_rlc_ue_entity::process_task (this=0x7ffe04939424, p_task=0x7ffe04e58020) at /root/DU/ran/DU_Alpha_Rel/src/du_app/gnb_mgr/bui
#8 0x000000000ad69f1 in gnb_du::gnb_du_worker_thread_instance::process_message (this=0x7ffe00402c24, p_task=0x7ffe04e58020, priority=2) at /root/DU/ran/DU_Alpha_Rel/src/du_app/gnb_mgr/build/./src/gnb_du_worker_thread.cpp:421
#9 0x000000000086f566 in ngp::thread_pool<gnb_du::gnb_du_worker_thread_instance, ssTskInfo>::thread_worker::run (this=0xa925280) at /root/DU/ran/DU_Alpha_Rel/src/du_app/gnb_mgr/build/./../include/ngp_thread_pool.h:334
#10 0x000000000ea24c7 in ngp::thread_entry_function (param=0xa925280) at /root/DU/ngp/thread/build/./src/ngp_sys_thread.cpp:110
#11 ngp::thread_start (param=0xa925280) at /root/DU/ngp/thread/build/./src/ngp_sys_thread.cpp:123
#12 0x00007ffff61e16ba in start_thread (arg=0x7ffe8c847700) at pthread_create.c:333
#13 0x00007ffff5f1741d in clone () at ../sysdeps/unix/sysv/linux/x86_64/clone.S:109
(gdb) p ptr
$1 = (Data **) 0x7ffe8c846b80
(gdb) p *ptr
$2 = (Data *) 0x0
(gdb) p dynMemElem->nextBktPtr
$3 = (CmMmEntry *) 0x0
(gdb)
```

历史记录

2025-08-25

- 状态从 新建 变更为 进行中

从已有log和挂死堆栈，只能判断出是RLC收到上行数据包处理中，post task到任务队列时，申请DU内部内存池，但内存池中内存结构已被破坏，发生了踩内存的情况。而无法知道踩内存发生在之前的那个环节。

先重新跑看看，如果能够持续复现，可以通过打开内存debug的log，观察具体是哪一个位置出现了内存越界访问。

#2 - 2023-06-27 15:55 - 匿名用户

- 状态从 进行中 变更为 挂起

待新版本出现问题后合并分析

#3 - 2023-12-05 14:57 - 郝雷

- 状态从 挂起 变更为 进行中

转测试

#4 - 2023-12-05 14:58 - 郝雷

在14P_pre1版本上，经马兰K项目现场验证，上行2天线大上行配置，10UE同时做总共300Mbps业务，跑2小时无挂死问题。

#5 - 2023-12-05 14:58 - 郝雷

- 状态从 进行中 变更为 已解决