

### 3.0基站产品测试 - 错误 #4964

#### [3.0产品测试] 4UE压力测试中，du出现挂死

2026-03-05 16:12 - 黄毅

状态:	进行中	开始日期:	2026-03-05
优先级:	一般	计划完成日期:	
指派给:	韩伟	% 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_3.2.1
发现问题版本:	Rel_3.2.1		

<b>描述</b> 测试版本：Rel3.2.1_Pre1T2版本 测试设备：军特整机192.168.8.234，网管：192.168.8.181 测试用例：4UE压力测试 基站配置：1D3U 测试终端：星创CPE*4 测试场景：基站启动正常，终端接入做上行业务。每个终端上行灌包100M 问题描述：压力测试中，du出现挂死
--

#### 历史记录

#1 - 2026-03-05 17:22 - 韩伟

- 文件 coredump调用栈信息.png 已添加
- 状态从新建变更为进行中

该问题已在定位修改中。目前看跑死位置

```
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  gnb_du::gnb_du_nrup_msg_comm::process_data_pdu (this=this@entry=0x7d20629a34, du_msg=du_msg@entry=0x7d25788434, pktNum=0x7dd1b29234, pktNum@entry=0x7dd1b29284, pktLen=0x7dd1b29230,
    pktLen@entry=0x7dd1b29280) at /home/zlw/du_push/ran/nr_hl_du/src/du_app/nrup/build/./src/gnb_du_nrup_msg_comm.cpp:235
235 /home/zlw/du_push/ran/nr_hl_du/src/du_app/nrup/build/./src/gnb_du_nrup_msg_comm.cpp: No such file or directory.
[Current thread is 1 (Thread 0x7dd1b29b70 (LWP 2335))]
(gdb) bt
#0  gnb_du::gnb_du_nrup_msg_comm::process_data_pdu (this=this@entry=0x7d20629a34, du_msg=du_msg@entry=0x7d25788434, pktNum=0x7dd1b29234, pktNum@entry=0x7dd1b29284, pktLen=0x7dd1b29230,
    pktLen@entry=0x7dd1b29280) at /home/zlw/du_push/ran/nr_hl_du/src/du_app/nrup/build/./src/gnb_du_nrup_msg_comm.cpp:235
#1  0x0000000000000000 in gnb_du::gnb_du_nrup_msg_comm::du_nrup_active_task (task_info=<optimized out>)
    at /home/zlw/du_push/ran/nr_hl_du/src/du_app/nrup/build/./src/gnb_du_nrup_msg_comm.cpp:118
#2  0x0000000000000000 in gnb_du::gnb_du_worker_thread_instance::process_message (this=0x7d20629a34, p_task=<optimized out>, priority=<optimized out>)
    at /home/zlw/du_push/ran/nr_hl_du/src/du_app/gnb_mgr/build/./src/gnb_du_worker_thread.cpp:512
#3  0x0000000000000000 in ngp::thread_pool::gnb_du::gnb_du_worker_thread_instance::start_thread (this=0xf490af0)
    at /home/zlw/du_push/ran/nr_hl_du/src/du_app/gnb_mgr/build/./.././.././../ngp/include/ngp_thread_pool.h:426
#4  0x0000000000000000 in thread_start () at /home/zlw/du_push/np/thread/build/./src/ngp_sys_thread.cpp:338
#5  0x0000000000000000 in start_thread (arg=0x7ffceef8ff) at pthread_create.c:486
#6  0x0000000000000000 in thread_start () at ../sysdeps/unix/sysv/linux/aarch64/clone.S:78
```

初步分析原因为：ue实例异常后继续被使用，直接导致挂死。

#2 - 2026-03-05 17:41 - 韩伟

- 文件 异常ue内存.png 已添加

异常ue实例进行解引用时挂死，一下为挂死ue实例内存情况：

```

(gdb) p dat_req
$32 = (gnb_du::nrup_dat_req_t *) 0x7d1f921730
(gdb) p *(gnb_du::nrup_dat_req_t *) 0x7d1f921730
$33 = {
  g_ue = 0x7d6e091830,
  sdu = 0x7d264dc630,
  lcType = 0 '\000',
  sduId = 0,
  rlcId = {
    rbId = 1 '\001',
    rbType = 0 '\000',
    ueId = 0,
    cellId = 0
  },
  hdr_len = 6 '\006',
  hdr_container = 0x7d454b903d ""
}
(gdb) p *(g_ue_t*)0x7d6e091830
$34 = {
  taskCb = 0x258,
  poolId = 0,
  crnti = 0,
  cellId = 0,
  reestCrnti = 45551584,
  reestCellId = 926299637,
  rrmUeCb = 0x3938373635343332,
  egtp_ue_ptr = 0x3736353433323130,
  nrupUeCb = 0x3534333231303938,
  appUeCb = 0x3332313039383736,
  rlcUlUeCb = 0x3130393837363534,
  rlcDlUeCb = 0x3938373635343332,
  nrupDlMsgQ = {
    read = 858927408,
    write = 926299444,
    size = 825243960,
    nReadFail = 892613426,
    nWriteFail = 959985462,
    n_write = 858927408,
    n_read = 926299444,
    data = 0x3938373635343332
  },
  rlcDlMsgQ = {
    read = 858927408,
    write = 926299444
  }
}

```

挂死在该消息，消息中挂载ue实例指针

该ue实例指针所指向内存已经被修改

#3 - 2026-03-05 17:42 - 韩伟

因为内存已经被修改，无法确定异常ue的rnti信息，暂无法确认该ue是否确实已经被释放了。

#4 - 2026-03-05 20:56 - 韩伟

- 文件 站上在线UE信息记录查询.png 已添加
- 文件 通过环形队列确认释放UE信息.png 已添加

通过corei记录信息，确认ue=0x7d6e09183确实已经释放  
 站上在线UE信息记录查询.png  
 通过环形队列确认释放UE信息.png  
 后通过core文件记录到的nrupDlMsgQ环形队列中信息，确认释放UE=0x7d6e091830的rnti为17116

#5 - 2026-03-05 20:57 - 韩伟

- 文件 UE\_17116\_释放Log.png 已添加

后再通过Log查找，找到17116终端确实在基站挂死前进行了释放：  
 UE\_17116\_释放Log.png

#6 - 2026-03-05 21:00 - 韩伟

基于这些信息，可以确认ue=17116已经放生了释放，但是消息队列中还缓存有该ue相关的消息待处理，在ue-17116释放后，ue实例内存释放后，缓存的消息在进行处理时，由于防护不到位，导致访问了已经释放的内存信息，直接导致挂死，针对此问题，对代码进行了修改和防护增强。

文件

20260305-160921.jpg	525 KB	2026-03-05	黄毅
core.WORKER_0_2.rar	45.7 MB	2026-03-05	黄毅

coredump调用栈信息.png	60.5 KB	2026-03-05	韩伟
异常ue内存.png	51.7 KB	2026-03-05	韩伟
站上在线UE信息记录查询.png	9.1 KB	2026-03-05	韩伟
通过环形队列确认释放UE信息.png	17.7 KB	2026-03-05	韩伟
UE_17116_释放Log.png	42.6 KB	2026-03-05	韩伟