# 3.0基站产品测试 - 错误 #4781

## Rel_3.1.5_Pre1T2版本16UE长保DU coredump

2026-01-23 16:38 - 郭 锁奇

| | | | |
|---|---|---|---|
| **状态:** | 审视 | **开始日期:** | 2026-01-23 |
| **优先级:** | 一般 | **计划完成日期:** | |
| **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_3.1.5 |
| **发现问题版本:** | Rel_3.1.5 | | |

**描述**

Rel_3.1.5_Pre1T2版本1D3U子帧配比上行双天线16UE上、下行udp灌包，CU coredump，定位后原因为RNTI最大个数配置。

### 历史记录

**#1 - 2026-01-26 15:16 - 郭 锁奇**

Rel_3.1.5_Pre1T2版本1D3U子帧配比上行双天线16UE上、下行udp灌包，DU coredump，定位后原因为ue释放挂死.

**#2 - 2026-01-29 21:00 - 韩 伟**

*- 状态 从 新建 变更为 进行中*

该问题已定位，挂死原因为ue释放流程中rel_trans定时器超时，访问待释放终端ueCb时，ueCb所在内存块已被释放，且内存已被其他点申请走，并进行了内存重写，因此挂死。

**#3 - 2026-01-30 09:28 - 韩 伟**

*- 文件 core_stack.png 已添加*

```
Program terminated with signal SIGSEGV, Segmentation fault.
#0  0x0000000000000000 in ?? ()
[Current thread is 1 (Thread 0x7dd46c2b70 (LWP 3940))]
(gdb) bt
#0  0x0000000000000000 in ?? ()
#1  0x00000000007a22ac in gnb_du::gnb_du_app_ue_msg_comm::send (this=this@entry=0x7d24629634, g_ue=g_ue@entry=0x7d54b9a830, msg=msg@entry=0x7d2984f134)
    at /home/zlw/du_push/ran/nr_hl_du/src/du_app/app_ue/build/../src/gnb_du_ue_msg_comm.cpp:234
#2  0x00000000007c4210 in gnb_du::gnb_ue_tmr::timer_expiry (tmrEvnt=<optimized out>, cb=<optimized out>, this=<optimized out>)
    at /home/zlw/du_push/ran/nr_hl_du/src/du_app/app_ue/build/../src/gnb_du_ue_tmr.cpp:311
#3  app_ue_tmr_expiry (cb=<optimized out>, tmrEvnt=<optimized out>) at /home/zlw/du_push/ran/nr_hl_du/src/du_app/app_ue/build/../src/gnb_du_ue_tmr.cpp:400
#4  0x00000000006a1c44 in cmnTmrExpiry (cb=<optimized out>, timer=0x7d26cdb164) at /home/zlw/du_push/ran/nr_hl_du/src/5gnr_cmn//cmn_gcb_hdl.c:441
#5  0x000000000067edd4 in cmPrcTmr (tqCp=0xe3e4e8 <cmGCb+70680>, tq=0xe3e448 <cmGCb+70520>, func=func@entry=0x6a1c00 <cmnTmrExpiry(unsigned long, cmTimer*)>)
    at /home/zlw/du_push/ran/nr_hl_du/src/cm/cm_bdy5.c:521
#6  0x00000000006a2364 in cmnHdlCmTmr (tskInfo=0x7d32a2d030) at /home/zlw/du_push/ran/nr_hl_du/src/5gnr_cmn//cmn_gcb_hdl.c:526
#7  0x00000000007cf480 in gnb_du::gnb_du_worker_thread_instance::process_message (this=0x7d24629f34, 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
#8  0x0000000000771370 in ngp::thread_pool<gnb_du::gnb_du_worker_thread_instance, ssTskInfo>::thread_worker::run (this=0x45174700)
    at /home/zlw/du_push/ran/nr_hl_du/src/du_app/gnb_mgr/build/../../../../../../ngp/include/ngp_thread_pool.h:426
#9  0x00000000008fc544 in thread_start () at /home/zlw/du_push/ngp/thread/build/../src/ngp_sys_thread.cpp:338
#10 0x0000007f8144d7e4 in start_thread (arg=0x7fd90501df) at pthread_create.c:486
#11 0x0000007f8107f70c in thread_start () at ../sysdeps/unix/sysv/linux/aarch64/clone.S:78
```

调用栈信息如上

**#4 - 2026-01-30 09:31 - 韩 伟**

*- 文件 异常终端.png 已添加*

```
  nsi_id = 0,
  trans_stop_ind_pres = false,
--Type <RET> for more, q to quit, c to continue without paging--
  cell_group_cfg = {
    <gnb_du::allocator> = {<No data fields>},
    members of gnb_du::du_ue_cell_group_cfg:
    ue_id = 17027,
    ue_mode = RGR_UE_CFG_SA_MODE,
    cell_group_id = 959985462,
    mac_cell_grp_cfg = {
      <gnb_du::allocator> = {<No data fields>},
      members of gnb_du::du_ue_mac_cell_group_cfg:
      mac_cell_group_cfg = {
        drx_cfg = {
          isDrxEnabled = 0 '\000',
          onDurTmrCfg = {
            tmrUnitTyp = 51 '3',
            t = {
              onDurTmrSubMs = 53 '5',
              onDurTmrMs = 13877
            }
          },
```

解堆栈，发现异常时终端为17027

#### #5 - 2026-01-30 09:37 - 韩 伟

*- 文件 rlf释放标记.png 已添加*

*- 文件 del_ue.png 已添加*

但是实际该终端对应的ueCb已经被RLF释放：

```
    at /home/zlw/du_push/ran/nr_hl_du/src/cm/cm_bdy5.c:521
#6  0x00000000006a2364 in cmnHdlCmTmr (tskInfo=0x7d32a2d030) at /home/zlw/du_push/ran/nr_hl_du/src/5gnr_cmn//cmn_gcb_hdl.c:526
#7  0x00000000007cf480 in gnb_du::gnb_du_worker_thread_instance::process_message (this=0x7d24629f34, p_task=<optimized out>, priority=
    at /home/zlw/du_push/ran/nr_hl_du/src/du_app/gnb_mgr/build/../src/gnb_du_worker_thread.cpp:512
#8  0x0000000000771370 in ngp::thread_pool<gnb_du::gnb_du_worker_thread_instance, ssTskInfo>::thread_worker::run (this=0x45174700)
    at /home/zlw/du_push/ran/nr_hl_du/src/du_app/gnb_mgr/build/../../../../../../ngp/include/ngp_thread_pool.h:426
#9  0x00000000008fc544 in thread_start () at /home/zlw/du_push/ngp/thread/build/../src/ngp_sys_thread.cpp:338
#10 0x0000007f8144d7e4 in start_thread (arg=0x7fd90501df) at pthread_create.c:486
#11 0x0000007f8107f70c in thread_start () at ../sysdeps/unix/sysv/linux/aarch64/clone.S:78
(gdb) f 1
#1  0x00000000007a22ac in gnb_du::gnb_du_app_ue_msg_comm::send (this=this@entry=0x7d24629634, g_ue=g_ue@entry=0x7d54b9a830, msg=msg@er
    at /home/zlw/du_push/ran/nr_hl_du/src/du_app/app_ue/build/../src/gnb_du_ue_msg_comm.cpp:234
234     /home/zlw/du_push/ran/nr_hl_du/src/du_app/app_ue/build/../src/gnb_du_ue_msg_comm.cpp: No such file or directory.
(gdb) p ueRlfReleased
$1 = {false <repeats 17025 times>, true, true, true, false, false, false, true, true, false <repeats 48503 times>}
(gdb)
```

```
#8  0x0000000000771370 in ngp::thread_pool<gnb_du::gnb_du_worker_thread_instance, ssTskInfo>::thread_worker::run (this=0x45174700)
    at /home/zlw/du_push/ran/nr_hl_du/src/du_app/gnb_mgr/build/../../../../../../ngp/include/ngp_thread_pool.h:426
#9  0x00000000008fc544 in thread_start () at /home/zlw/du_push/ngp/thread/build/../src/ngp_sys_thread.cpp:338
#10 0x0000007f8144d7e4 in start_thread (arg=0x7fd90501df) at pthread_create.c:486
#11 0x0000007f8107f70c in thread_start () at ../sysdeps/unix/sysv/linux/aarch64/clone.S:78
(gdb) f 1
#1  0x00000000007a22ac in gnb_du::gnb_du_app_ue_msg_comm::send (this=this@entry=0x7d24629634, g_ue=g_ue@entry=0x7d54b9a830, msg=msg@entry=0x7d2984f134)
    at /home/zlw/du_push/ran/nr_hl_du/src/du_app/app_ue/build/../src/gnb_du_ue_msg_comm.cpp:234
234     /home/zlw/du_push/ran/nr_hl_du/src/du_app/app_ue/build/../src/gnb_du_ue_msg_comm.cpp: No such file or directory.
(gdb) p cmGCb
value of type `CmGCb' requires 71216 bytes, which is more than max-value-size
(gdb) p cmGCb.ueLstCp
$1 = {0x7d6a26d830, 0x7d619f4030, 0x7d585e1830, 0x7d3ac33830, 0x7d695ec830, 0x7d72425030, 0x7d55a08830, 0x7d376af030, 0x0, 0x0, 0x0, 0x7d67885830, 0x7d39060830, 0x7d3cb27030, 0x7d49316030,
  0x0 <repeats 1185 times>}
(gdb) p cmGCb.startCrnti
$2 = 17017
```

#### #6 - 2026-01-30 09:37 - 韩 伟

*- 文件 rel_trans_event.png 已添加*

所以在rel_trans定时器超时释放ueCb时异常：

```
(gdb) p *(gnb_du::gnb_du_message *) 0x7d2984f134
$3 = {
  <gnb_du::allocator> = {<No data fields>},
  members of gnb_du::gnb_du_message:
  _vptr.gnb_du_message = 0xa77ec0 <vtable for gnb_du::gnb_du_message+16>,
  ref_cnt = 0,
  msg_hdr = {
    poolId = 0,
    srcEntType = SS_CMN_TMR,
    dstEntType = SS_APP_UE,
    event = 123,
    reserved = 0,
    reserved1 = 0,
    reserved2 = 5720896438272,
    reserved3 = 0,
    msgLen = 668316976,
    startTick = 6994439831644274813,
    middleTick = 349610337894400,
    endTick = 281470681743360
  },
  msg = 0x7d26cdb134,
  trans_id = 0
}
(gdb)
```

#### #7 - 2026-01-30 09:41 - 韩 伟

通过对代码分析，存在在竞争解决释放情况下提前删除ueCb,且rel_trans定时器不感知，且是在超时后去使用了已被释放的内存。针对此情况一方面增加rel_trans异常保护，另一方面对异常释放流程进行修改。修改已合入。

#### #8 - 2026-02-03 09:30 - 韩 伟

*- 状态 从 进行中 变更为 审视*

*- 指派给 从 韩 伟 变更为 周 立伟*

### 文件

| | | | |
|---|---|---|---|
| core_stack.png | 49.1 KB | 2026-01-30 | 韩 伟 |
| 异常终端.png | 15.7 KB | 2026-01-30 | 韩 伟 |
| rlf释放标记.png | 34.6 KB | 2026-01-30 | 韩 伟 |
| del_ue.png | 32 KB | 2026-01-30 | 韩 伟 |
| rel_trans_event.png | 20.6 KB | 2026-01-30 | 韩 伟 |