

B5G_UE - 错误 #5085

【B5g_ue】V0.0.1_T07__Alpha16,终端90接入过程core dump

2026-03-30 10:27 - 周磊

状态:	已关闭	开始日期:	2026-03-30
优先级:	一般	计划完成日期:	
指派给:	周磊	% 完成:	0%
类别:		预期时间:	0.00 小时
目标版本:		耗时:	0.00 小时

描述

【B5g_ue】V0.0.1_T07__Alpha16,终端90接入过程core dump

测试环境：基站30+终端90

问题描述：【B5g_ue】V0.0.1_T07__Alpha16,终端90接入过程core dump，RLC异常，已合入 17，待回归验证

```
[DEBUG]:Memory Section - [MSG_DDR_MEM]: Base Address: [0x7edc000000]; Maximum Size: [134217728]
[DEBUG]:Memory Section - [MSG_DDR_MEM]: Variable Name: [dIAddr]; Allocated Address: [0x7edd860000]; Allocated Size: [5242880]
[DEBUG]:Memory Section - [MSG_DDR_MEM]: Base Address: [0x7edc000000]; Maximum Size: [134217728]
[DEBUG]:Memory Section - [MSG_DDR_MEM]: Variable Name: [uIAddr]; Allocated Address: [0x7eddd60000]; Allocated Size: [2621440]
msg_transfer_init is success !!!
[DEBUG]:Memory Section - [MSG_DDR_MEM]: Base Address: [0x7edc000000]; Maximum Size: [134217728]
[DEBUG]:Memory Section - [MSG_DDR_MEM]: Variable Name: [dIAddr]; Allocated Address: [0x7eddf60000]; Allocated Size: [655360]
[DEBUG]:Memory Section - [MSG_DDR_MEM]: Base Address: [0x7edc000000]; Maximum Size: [134217728]
[DEBUG]:Memory Section - [MSG_DDR_MEM]: Variable Name: [uIAddr]; Allocated Address: [0x7ede080000]; Allocated Size: [1310720]
msg_transfer_init is success !!!
handIdOam 66048
[DEBUG]:core[0x0000000c] send handshake request message,value[0x5a5a5a66].
[DEBUG]:core[0x0000000c] recieved handshake response message,value[0xa5a5a5b1].
ucp_handshake is success!!!
clkMode is :1,start to sync gpswill get gps sync status.
.....[DEBUG]:stc tracking ok !!!!! maintain g_sys_time:1774578044

sync_flag=1,set sync to cp
.GPS sync ok,set tod_incr_en
.GPS sync ok,set sync to 12
.
gps sync ok.
Thread threadL3 priority: 0, policy:0, cpuid:2 sockId:0
Thread T2 priority: 0, policy:0, cpuid:5 sockId:0
Thread T3 priority: 0, policy:0, cpuid:4 sockId:0
Thread T4 priority: 0, policy:0, cpuid:7 sockId:0
Thread T5 priority: 0, policy:0, cpuid:1 sockId:0
Thread T6 priority: 0, policy:0, cpuid:6 sockId:0
Thread ReceiveFromLlc priority: 0, policy:0, cpuid:3
DRB Established = 1
Rrc Switch node type to UE
./start.sh: line 13: 418 Segmentation fault (core dumped) ./build/psarmapp -l 0-7
root@driver:~#
```

历史记录

#1 - 2026-03-31 09:32 - 王艳芳

- 状态从新建变更为进行中

【问题原因】从终端LOG显示，RRC先后发起了RLC_SUSPEND和RLC_RELEASE，RLC_SUSPEND使RLC实体释放了激活列表，转入了非激活列表，而RLC_RELEASE的原实现是释放激活列表，由于激活列表已经释放，所以引发CRASH。

【解决方案】优化完善RLC_RELEASE的实现

【测试结果】问题已解决

#2 - 2026-04-01 16:03 - 李常

- 状态从进行中变更为审视

- 指派给从王艳芳变更为李常

修改合理，已入版本V0.0.1_T07__Alpha17。

#3 - 2026-04-01 16:04 - 李常

- 状态从 审视 变更为 转测试

- 指派给从 李常 变更为 周磊

#4 - 2026-04-10 14:27 - 周磊

更新版本后，多次测试，未出现挂死

#5 - 2026-04-10 14:27 - 周磊

- 状态从 转测试 变更为 已解决

#6 - 2026-04-10 14:27 - 周磊

- 状态从 已解决 变更为 已关闭

文件

20260330-102724.jpg

626 KB

2026-03-30

周磊