

B5G_UE - 错误 #5181

【B5g_ue】V0.0.1_T07__Alpha20,终端接入，打印RRC Release start!后挂死

2026-04-20 12:17 - 周磊

状态:	转测试	开始日期:	2026-04-20
优先级:	高	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__Alpha20,终端接入，打印RRC Release start!后挂死

测试环境：基站30+终端90

问题描述：V0.0.1_T07__Alpha20,终端接入，打印RRC Release start!后挂死

RRC Release start!
./start.sh: line 13: 417 Killed ./build/psarmapp -l 0-7

```
msg_transfer_init is success !!!
[DEBUG]:Memory Section - [MSG_DDR_MEM]: Base Address: [0x7eac000000]; Maximum Size: [134217728]
[DEBUG]:Memory Section - [MSG_DDR_MEM]: Variable Name: [dIAddr]; Allocated Address: [0x7eadfe0000]; Al
located Size: [655360]
[DEBUG]:Memory Section - [MSG_DDR_MEM]: Base Address: [0x7eac000000]; Maximum Size: [134217728]
[DEBUG]:Memory Section - [MSG_DDR_MEM]: Variable Name: [uIAddr]; Allocated Address: [0x7eae000000]; Al
located Size: [1310720]
msg_transfer_init is success !!!
handId0am 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:1776655474
sync_flag=1,set sync to cp
.GPS sync ok,set tod_incr_en
.GPS sync ok,set sync to l2
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 T6 priority: 0, policy:0, cpuid:6 sockId:0
Thread T4 priority: 0, policy:0, cpuid:7 sockId:0
Thread T5 priority: 0, policy:0, cpuid:1 sockId:0
Thread ReceiveFromIc priority: 0, policy:0, cpuid:3
DRB Established = 1
Rrc Switch mode type to UE
logfile: /run/yz_zlog_20260420032535.log
logfile: /run/yz_zlog_20260420032633.log
logfile: /run/yz_zlog_20260420032731.log
logfile: /run/yz_zlog_20260420032829.log
logfile: /run/yz_zlog_20260420032926.log
RRC Release start!
./start.sh: line 13: 417 Killed                   ./build/psarmapp -l 0-7
root@driver:~#
```

```
[ 5] 1060.00-1061.00 sec 0.00 Bytes 0.00 bits/sec 0.275 ms 0/0 (0%)
[ 5] 1061.00-1062.00 sec 0.00 Bytes 0.00 bits/sec 0.275 ms 0/0 (0%)
[ 5] 1062.00-1063.00 sec 0.00 Bytes 0.00 bits/sec 0.275 ms 0/0 (0%)
[ 5] 1063.00-1064.00 sec 0.00 Bytes 0.00 bits/sec 0.275 ms 0/0 (0%)
[ 5] 1064.00-1065.00 sec 0.00 Bytes 0.00 bits/sec 0.275 ms 0/0 (0%)
[ 5] 1065.00-1066.00 sec 0.00 Bytes 0.00 bits/sec 0.275 ms 0/0 (0%)
[ 5] 1066.00-1067.00 sec 0.00 Bytes 0.00 bits/sec 0.275 ms 0/0 (0%)
[ 5] 1067.00-1068.00 sec 0.00 Bytes 0.00 bits/sec 0.275 ms 0/0 (0%)
[ 5] 1068.00-1069.00 sec 0.00 Bytes 0.00 bits/sec 0.275 ms 0/0 (0%)
[ 5] 1069.00-1070.00 sec 0.00 Bytes 0.00 bits/sec 0.275 ms 0/0 (0%)
[ 5] 1070.00-1071.00 sec 0.00 Bytes 0.00 bits/sec 0.275 ms 0/0 (0%)
[ 5] 1071.00-1072.00 sec 0.00 Bytes 0.00 bits/sec 0.275 ms 0/0 (0%)
[ 5] 1072.00-1073.00 sec 0.00 Bytes 0.00 bits/sec 0.275 ms 0/0 (0%)
[ 5] 1073.00-1074.00 sec 0.00 Bytes 0.00 bits/sec 0.275 ms 0/0 (0%)
[ 5] 1074.00-1075.00 sec 0.00 Bytes 0.00 bits/sec 0.275 ms 0/0 (0%)
[ 5] 1075.00-1076.00 sec 0.00 Bytes 0.00 bits/sec 0.275 ms 0/0 (0%)
[ 5] 1076.00-1077.00 sec 0.00 Bytes 0.00 bits/sec 0.275 ms 0/0 (0%)
[ 5] 1077.00-1078.00 sec 0.00 Bytes 0.00 bits/sec 0.275 ms 0/0 (0%)
[ 5] 1078.00-1079.00 sec 0.00 Bytes 0.00 bits/sec 0.275 ms 0/0 (0%)
[ 5] 1079.00-1080.00 sec 0.00 Bytes 0.00 bits/sec 0.275 ms 0/0 (0%)
[ 5] 1080.00-1081.00 sec 0.00 Bytes 0.00 bits/sec 0.275 ms 0/0 (0%)
^C[ 5] 1081.00-1081.66 sec 0.00 Bytes 0.00 bits/sec 0.275 ms 0/0 (0%)
-----
[ ID] Interval           Transfer        Bitrate        Jitter        Lost/Total Datagram
[ 5] 0.00-1081.66 sec 6.40 GBytes 50.8 Mbits/sec 0.275 ms 880253/6164875 (14
iver
iperf3: interrupt - the server has terminated
yzrt@yzrt:~$ ^C
yzrt@yzrt:~$ ^C
yzrt@yzrt:~$ ^C
yzrt@yzrt:~$ ^C
yzrt@yzrt:~$ ^C
yzrt@yzrt:~$ iperf3 -s
Server listening on 5201
-----
^Ciperf3: interrupt - the server has terminated
yzrt@yzrt:~$ ^C
yzrt@yzrt:~$ ^C
yzrt@yzrt:~$ ^C
yzrt@yzrt:~$
```

```
2. 192.168.2.90 (root) x
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "aarch64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word" ...
Reading symbols from ./build/psarmapp ... done.
[New LWP 496]
[New LWP 439]
[New LWP 453]
[New LWP 494]
[New LWP 493]
[New LWP 438]
[New LWP 497]
[New LWP 498]
[New LWP 495]
[New LWP 589]
[New LWP 491]
[New LWP 591]
[New LWP 492]
[New LWP 590]
[New LWP 500]
[New LWP 454]
[New LWP 456]
[New LWP 455]
[New LWP 499]
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/aarch64-linux-gnu/libthread_db.so.1".
Core was generated by './build/psarmapp -l 0-7'.
Program terminated with signal SIGSEGV, Segmentation fault.
#0 0x0000000000a28e9c in wnUeHRLcTxCP (rlcCb=0x15afe8880) at src/l2/rlc/csrc/wn5gNrUePsHRLcTx.c:312
312   src/l2/rlc/csrc/wn5gNrUePsHRLcTx.c: No such file or directory.
[Current thread is 1 (Thread 0x7f8cff7900 (LWP 496))]
(gdb) bt
#0 0x0000000000a28e9c in wnUeHRLcTxCP (rlcCb=0x15afe8880) at src/l2/rlc/csrc/wn5gNrUePsHRLcTx.c:312
#1 0x0000000000a3cd68 in wnT3PollCpMsgs (pdcpRlcCb=<optimized out>) at src/l2/pdcp/csrc/wn5gNrUePsUPdcpTx.c:124
#2 0x000000000083c4cc in T3 (ueCb=0x30c3ac30) at src/ueapp/csrc/wn5gNrUePsUeApp.c:400
#3 0x0000000000db9990 in eal_thread_loop ()
#4 0x00000007f96ea87e4 in start_thread (arg=0x7ffcd9ba5f) at pthread_create.c:486
#5 0x00000007f96d2e70c in thread_start () at ../sysdeps/unix/sysv/linux/aarch64/clone.S:78
(gdb) f 0
#0 0x0000000000a28e9c in wnUeHRLcTxCP (rlcCb=0x15afe8880) at src/l2/rlc/csrc/wn5gNrUePsHRLcTx.c:312
312   in src/l2/rlc/csrc/wn5gNrUePsHRLcTx.c
(gdb) p rlcCb->rlcMacCb->macCb->ueCb
Cannot access memory at address 0x15afe8e78
(gdb) p rlcCb->rlcMacCb->macCb
Cannot access memory at address 0x15afe8e78
(gdb) p rlcCb->rlcMacCb
Cannot access memory at address 0x15afe8e78
(gdb) p rlcCb
$1 = (wnRlcCbP) 0x15afe8880
(gdb) █
```

历史记录

#1 - 2026-04-20 15:21 - 李常

- 状态从 新建 变更为 进行中

- 指派给从 李常 变更为 b jz

#2 - 2026-04-21 13:48 - 李常

- 优先级从 一般 变更为 高

#3 - 2026-04-22 10:19 - b jz

- 文件 PixPin_2026-04-22_10-18-08.png 已添加

- 状态从 进行中 变更为 审视

- 指派给从 b jz 变更为 李常

修改释放流程，支持反复释放接入。

```
Thread ReceiveFromL1c priority: 0, policy:0, cpuid:3
DRB Established = 1
Rrc Switch node type to IRN
RRC Release start!
Rrc Switch node type to OC-UE
Rrc release OC-UE state
DRB Established = 1
Rrc Switch node type to IRN
RRC Release start!
Rrc Switch node type to OC-UE
Rrc release OC-UE state
DRB Established = 1
Rrc Switch node type to IRN
RRC Release start!
Rrc Switch node type to OC-UE
Rrc release OC-UE state
DRB Established = 1
Rrc Switch node type to IRN
RRC Release start!
Rrc Switch node type to OC-UE
Rrc release OC-UE state
DRB Established = 1
Rrc Switch node type to IRN
RRC Release start!
Rrc Switch node type to OC-UE
Rrc release OC-UE state
```

#4 - 2026-04-23 14:32 - 李常

问题原因：当终端第二次从ouce转到IRN后，基站发起release，终端就挂死（之前代码中rrc release流程处理不完善，目前将这种场景修改完善后，自测10次左右无dump）。修改合理，计划合入下一个版本。

#5 - 2026-04-24 16:05 - 李常

- 状态从 审视 变更为 转测试
- 指派给从 李常 变更为 周磊

已合入到V0.0.1_T07__Alpha21版本中，请负责验证。

文件

20260420-121500.jpg	973 KB	2026-04-20	周磊
20260420-121545.jpg	355 KB	2026-04-20	周磊
PixPin_2026-04-22_10-18-08.png	113 KB	2026-04-22	b jz